UPS Network Management Card - Network-M2

User guide

English

1.6.6

1 Table of Contents

2 Contextual Help

2.1 Login page

The page language is set to English by default but can be switched to browser language when it is managed.
After navigating to the assigned IP address, accept the untrusted certificate on the browser.

2.1.1 Logging in for the first time

1. Enter default password

As you are logging into the Network Module for the first time you must enter the factory set default username and password.

- Username = admin
- Password = admin

2. Change default password

Changing the default password is mandatory and requested in a dedicated window.

Enter your current password first, and then enter the new password twice.

Follow the password format recommendations on the tooltip in order to define a secure password.

3. Accept license agreement

On the next step, License Agreement is displayed.

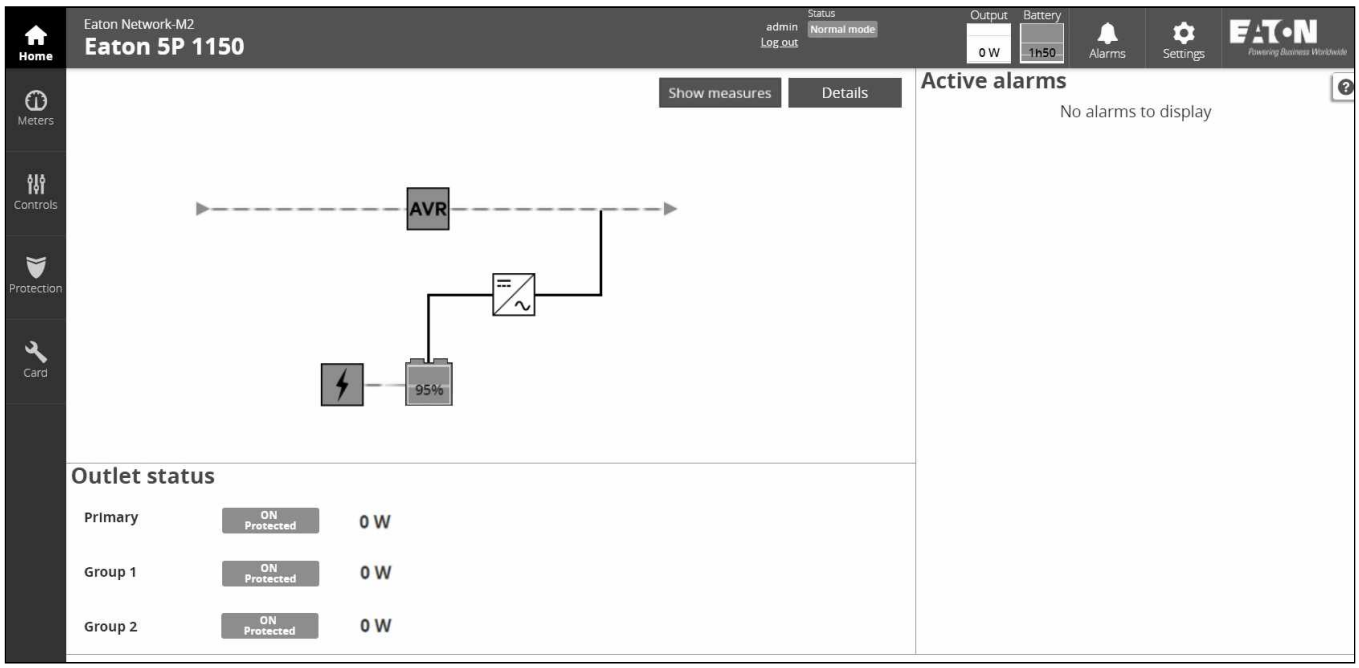
Read and accept the agreement to continue.

2.1.2 Troubleshooting login issues

For details on troubleshooting, see the ***Troubleshooting*** section.

2.2 Home

The Home screen provides status information for the device including synoptic diagrams, key measures and active alarms.



2.2.1 Menu structure

Button	Description
Home	*Overview and status of UPS Module:* • *Synoptic* • *Active alarms* • *Outlet status*
Settings	*Module settings:* • *General* • *Date & Time* • *Users* • *Network* • *Protocols* • *SNMP* • *Certificates* • *Email* • *My preferences*
Alarms	*List of alarms with date and time:* • *Details* • *Clear* • *Export*

Meters	*Power:* • *Frequency* • *Voltage* • *Current* • *Power* *Battery:* • *Overview* • *Details* • *Test* *Measure logs:* • *Configuration* • *Measure logs*
Controls	*Control of:* • *Entire UPS* • *Outlets*
Protection	• *Scheduled shutdown* • *Agent list* • *Agent settings* • *Power outage policy*
Sensors*	• *Status* • *Alarm configuration* • *Information*
Card	• *System information* • *System logs* • *Administration* • *Commissioning (Sensors)*

* Displayed when sensors are commissioned in Card menu.

2.2.2 Energy flow diagram

Line interactive

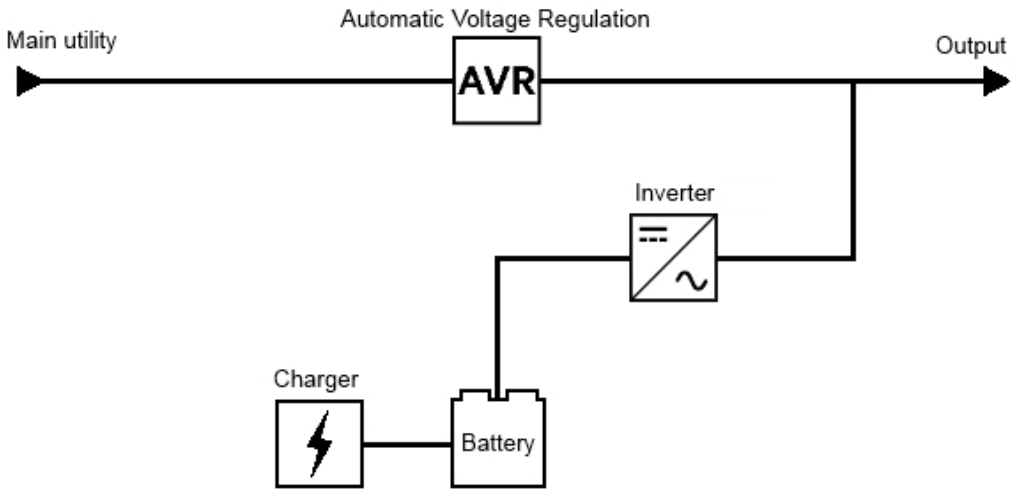
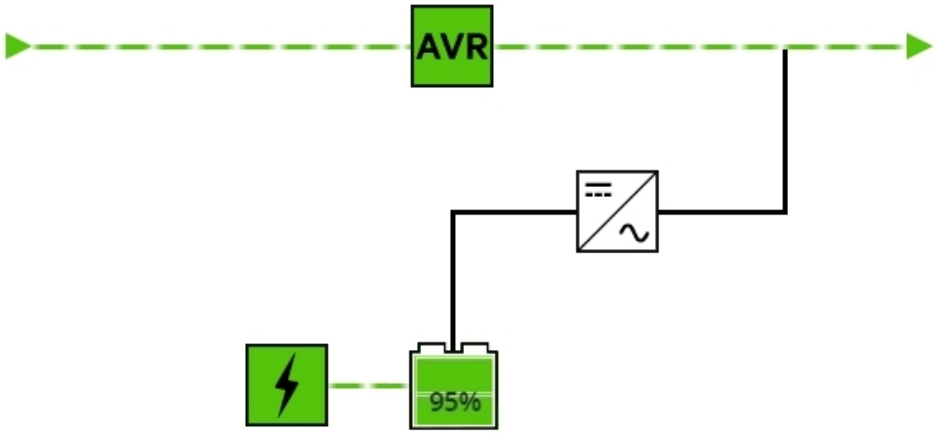
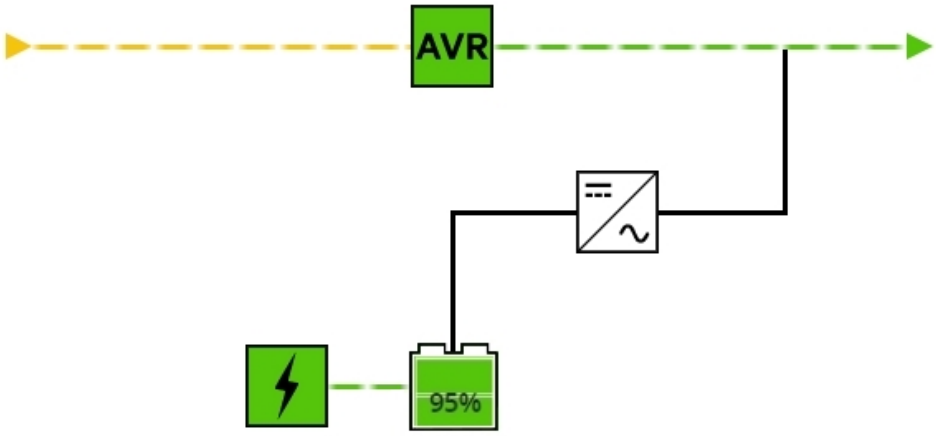


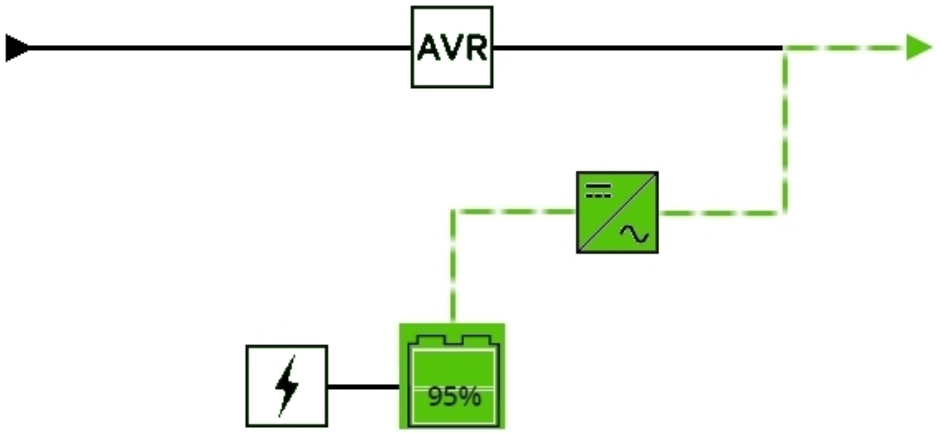
Diagram elements description

Symbols	Description	Possible states			
		Green	**Yellow**	**Red**	**Black / White / Greyed**
	Main utility	Powered	Out of nominal range		Not present Unknown
AVR	The equipment is protected and powered through an **AVR** device.	Normal mode Buck mode Boost mode	In overload		Not powered Unknown
	Output of the UPS.	Protected	In overload Not protected	In short circuit	Not powered Unknown
	Internal battery **charger**.	Charging Floating		In fault	Resting Not powered Unknown
	Battery for the backup power.	Powering the load	End of life	In fault Not present	Not used to power the load Unknown

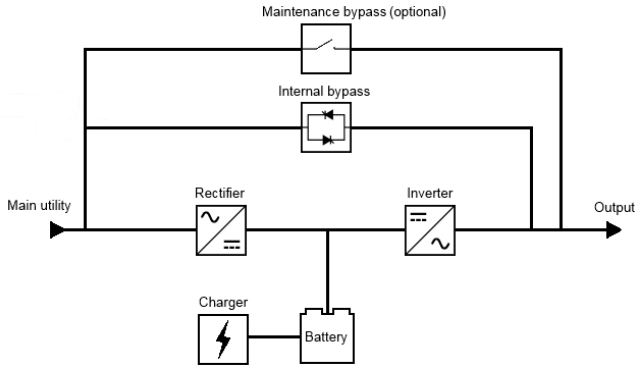
	**Battery level**	> 50% and > low battery threshold (Settable on the UPS)	< 50% and > low battery threshold (Settable on the UPS)	< Below low battery threshold (Settable on the UPS)	
	**Inverter**: convert DC power to AC power.	Powered	In overload	In short circuit In fault	Not powered Unknown
	Wiring	Energy flow	In overload Out of nominal range		No energy Unknown

Line interactive diagram examples

Normal mode	
Buck/Boost mode	

Battery mode	

Online



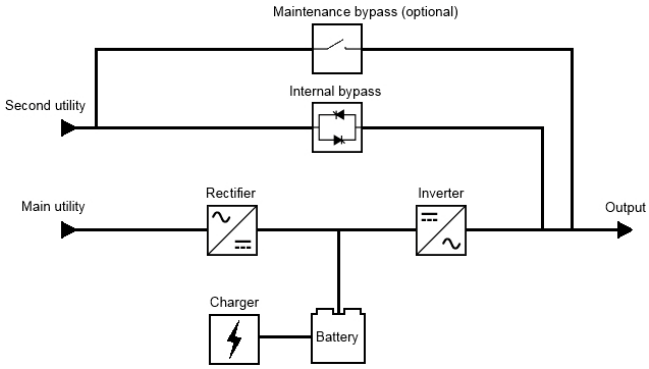
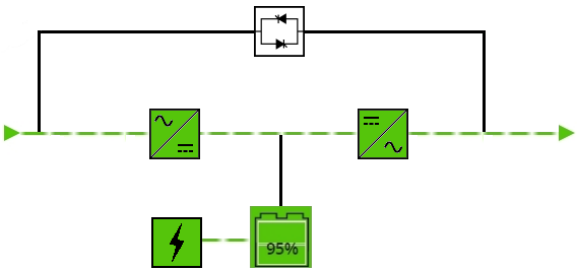
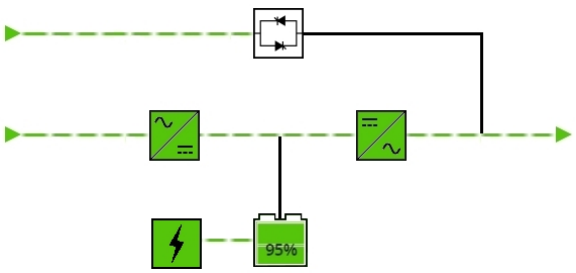
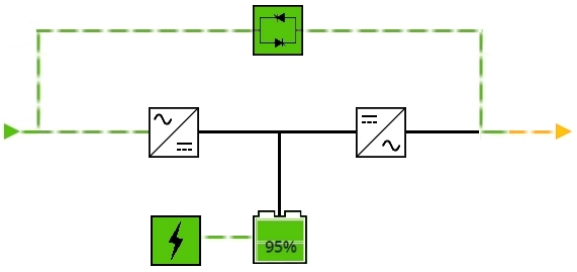
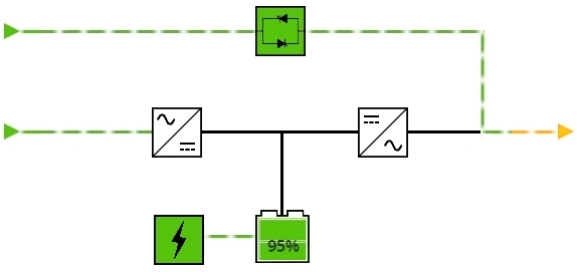


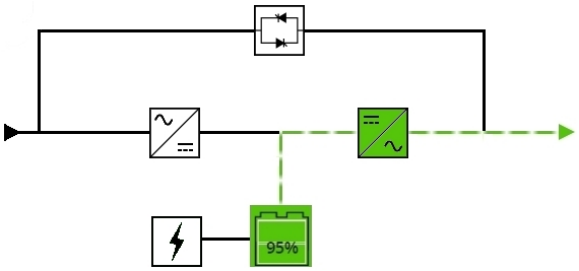
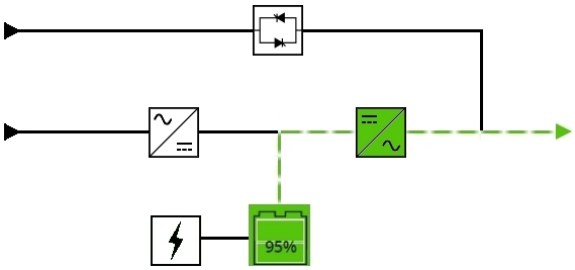
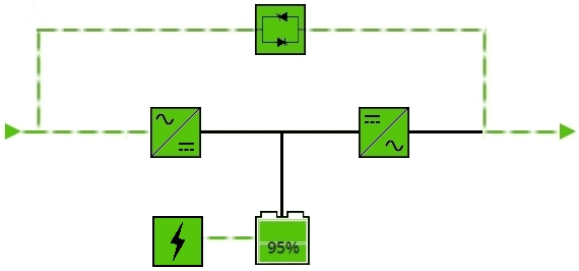
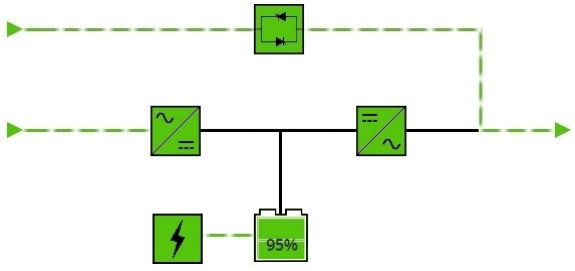
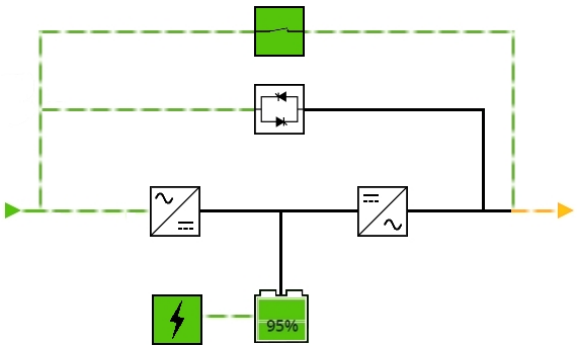
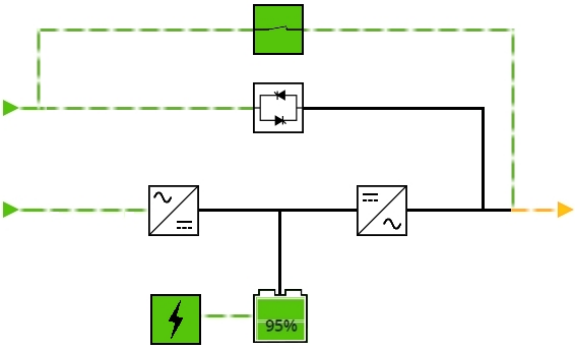
Diagram elements description

Symbols	Description	Possible states			
		Green	**Yellow**	**Red**	**Black or white**
	Main utility or **second utility**	Powered	Out of nominal range		Not present Unknown
	Rectifier: convert AC power to DC power.	Powered HE mode (ready)	In overload	In short circuit In fault	Not powered Unknown
	Inverter: convert DC power to AC power.	Powered HE mode (ready)	In overload	In short circuit In fault	Not powered Unknown
	Output of the UPS.	Protected	In overload Not protected	In short circuit	Not powered Unknown
	Internal battery **charger**.	Charging Floating		In fault	Resting Not powered Unknown

	Battery for the backup power.	Powering the load	End of life	In fault Not present	Not used to power the load Unknown
	Battery level	> 50% and > low battery threshold (Settable on the UPS)	< 50% and > low battery threshold (Settable on the UPS)	< Below low battery threshold (Settable on the UPS)	
	Automatic bypass	Powered (standby, auto bypass, forced bypass, high efficiency mode)	In overload	In fault	Not powered Unknown
	Maintenance bypass (optional)	Powered (maintenance bypass)			Not powered Unknown
	Wiring	Energy flow	In overload Out of nominal range		No energy Unknown

Online diagram examples

	Single input source	**Dual input sources**
Online mode		
Bypass mode		

Battery mode		
HE mode		
Maintenance bypass mode		

2.2.3 Top bar

Card name – Displays the card name

UPS name – Displays by default the UPS model or the system name if filled in the section Card>>>System information>>>System name

Current user – Displays current user name

Logout – Logs the current user out by destroying the current user session

Status – Provides device (example UPS) status information

Output power – Provides output power status information

Battery status – Provides battery status information

Alarms button – Open alarm page

Settings button – Open settings page

2.2.4 Details

This view provides a summary of device identification information and nominal values:

Name

Model

P/N

S/N

Location

Firmware version

Input Voltage

Input Frequency

Output Voltage

Output Frequency

The **COPY TO CLIPBOARD** button will copy the information to your clipboard so that it can be past.

For example, you can copy and paste information into an email.

2.2.5 Show measures

Provides input and output measures on the synoptic.

Example #1:

- Single input source
- 1 phase in
- 1 phase out

Input measures	Output measures
Voltage (V) Current (A) Frequency (Hz)	Voltage (V) Current (A) Frequency (Hz)

Example #2:

Dual input sources

- 3 phases in
- 3 phases out

Input measures (main and secondary)			Output measures		
Phase #1 Voltage (V) Current (A)	Phase #2 Voltage (V) Current (A)	Phase #3 Voltage (V) Current (A)	Phase #1 Voltage (V) Current (A)	Phase #2 Voltage (V) Current (A)	Phase #3 Voltage (V) Current (A) Load (W) Load (%)
Frequency (Hz)			Frequency (Hz)		

2.2.6 Outlet status

Provides the status of the UPS outlets (ON/OFF) by load segmentation:

Status (ON/OFF— Protected/Not protected/Not powered)

Load level (W) – availability depending on the UPS model

Shutdown countdown

Startup countdown

Note: Load segmentations allow non-priority equipment to automatically power down during an extended power outage to keep battery runtime on essential equipment.

This feature is also used to remote reboot and sequential start servers to restrict inrush currents.

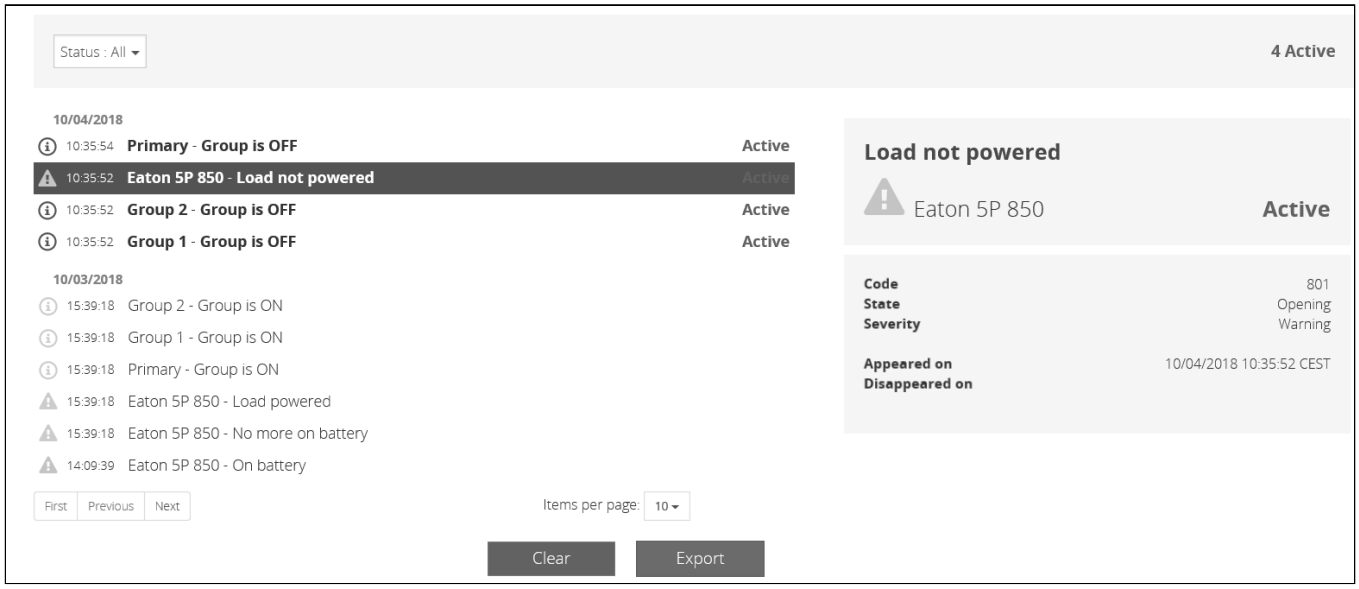
2.2.7 Active Alarms

Only active alarms are displayed, the Alarms icon will also display the number of active alarms.

Alarms are sorted by date, alert level, time, and description.

Note: To see the alarm history, press the **Alarms** button.

2.3 Alarms



2.3.1 Alarm sorting

Alarms can be sorted by selecting:

- All
- Active only

2.3.2 Alarm details

All alarms are displayed and sorted by date, with alert level, time, description, and status.

Example:

	Active	Opened	Closed
Info	10:55:49 **Group 1 - Group is OFF** Active	10:35:52 Group 1 - Group is OFF	10:54:23 Group 1 - Group is ON
Warning	10:55:47 **Eaton 5P 850 - Load not powered** Active	10:35:52 Eaton 5P 850 - Load not powered	10:54:12 Eaton 5P 850 - Load powered

Critical	10:55:47 **Eaton 5P 850 - No battery** **Active**	11:11:13 Eaton 5P 850 - No battery	11:11:49 Eaton 5P 850 - Battery present

2.3.3 Alarm paging

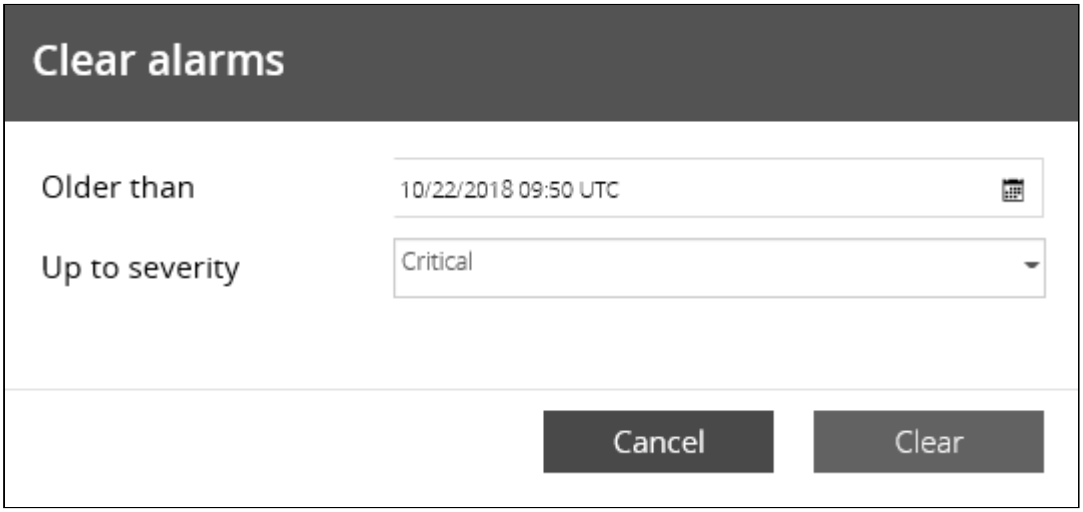
The number of alarms per page can be changed (10-15-25-50-100).

When the number of alarms is above the number of alarms per page, the buttons **First**, **Previous** and **Next** appears to allow navigation in the Alarm list.

2.3.4 Alarm export

Press the **Export** button to download the file.

2.3.5 Clear alarm logs



Press the **Clear** button to clear alarms that are older than a specified date and up to a defined severity.

2.3.6 Alarm list with codes

For details on alarm codes, see the ***Information>>>Alarm log codes*** section.

2.4 Settings

2.4.1 General

Location

Text field that is used to provide the card location information.

Card system information is updated to show the defined location.

Contact

Text field that is used to provide the contact name information.

Card system information is updated to show the contact name.

System name

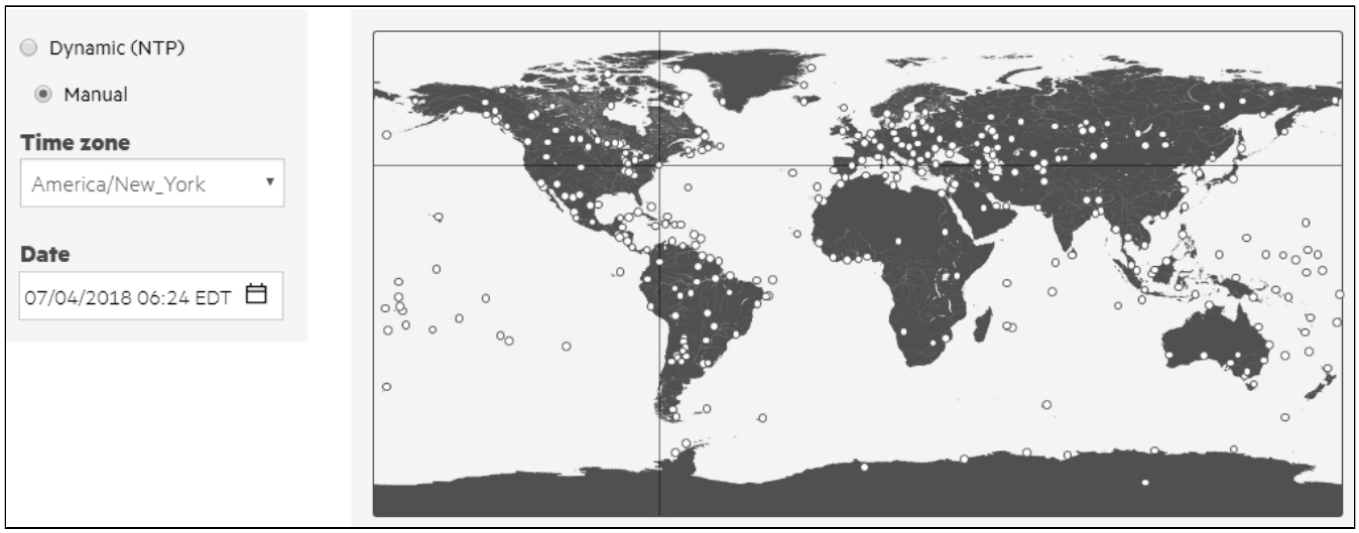
Text field that is used to provide the system name information.

Card system information is updated to show the system name.

Default settings parameters and limitations

For details on default parameters and limitations, see the ***Information>>>Default settings parameters*** section.

2.4.2 Date & Time



The current date and time appears in the footer at the bottom of the screen.

You can set the time either manually or automatically.

Manual: Manually entering the date and time

1. Select the time zone for your geographic area from the time zone pull-down menu or with the map.
2. Select the date and time.
3. Save the changes.

Dynamic (NTP): Synchronizing the date and time with an NTP server

1. Enter the IP address or host name of the NTP server in the NTP server field.
2. Select the time zone for your geographic area from the time zone pull-down menu or with the map.
3. Save the changes.

Note:

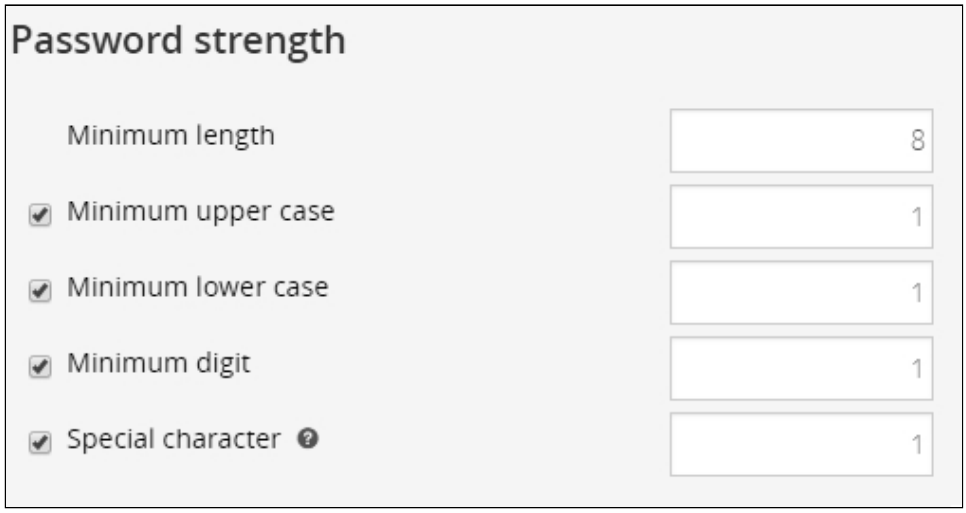
DST is managed based on the time zone.

Default settings parameters and limitations

For details on default parameters and limitations, see the ***Information>>>Default settings parameters*** section.

2.4.3 Users

Password strength rules



To set the password strength rules, apply the following restrictions:

- Minimum length
- Minimum upper case
- Minimum lower case
- Minimum digit
- Special character

Press **Save** after modifications.

Account expiration

To set the account expiration rules, apply the following restrictions:

- Password expires after (in days).

  The main administrator password never expires.

> ⚠
>
> 1. If this feature is disabled, the administrator account can be locked after the password expiration.
> 2. If Enabled, the administrator password never expires, make sure it is changed regularly.

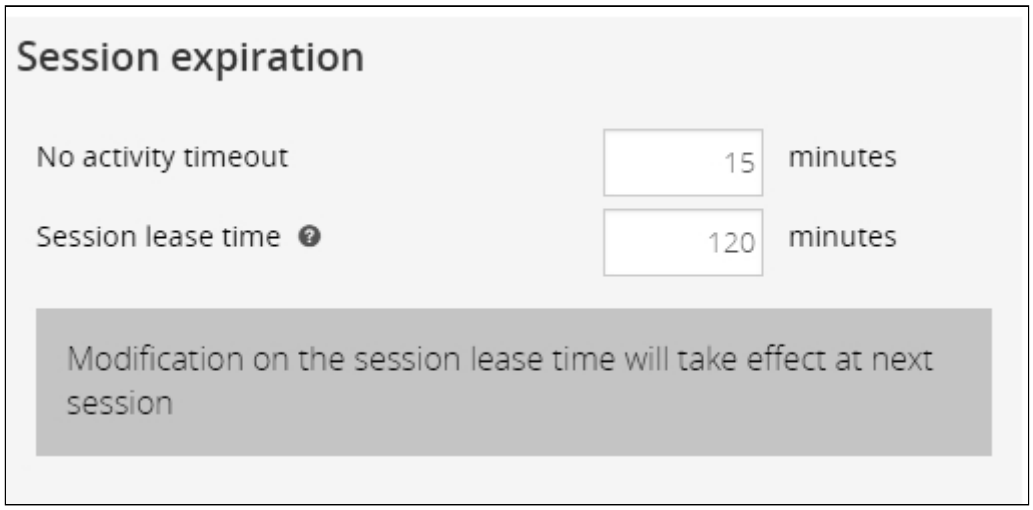
- Block account when invalid password is entered after (in number of attempts).

  The main administrator account will never block.

> ⚠
>
> 1. If this feature is disabled, the administrator account can be locked after the number of failed connections defined.
> 2. If Enabled, the security level of the administrator account is reduced because unlimited password entry attempts are allowed.

Press **Save** after modifications.

Session expiration



To set the session expiration rules, apply the following restrictions:

- No activity timeout (in minutes).

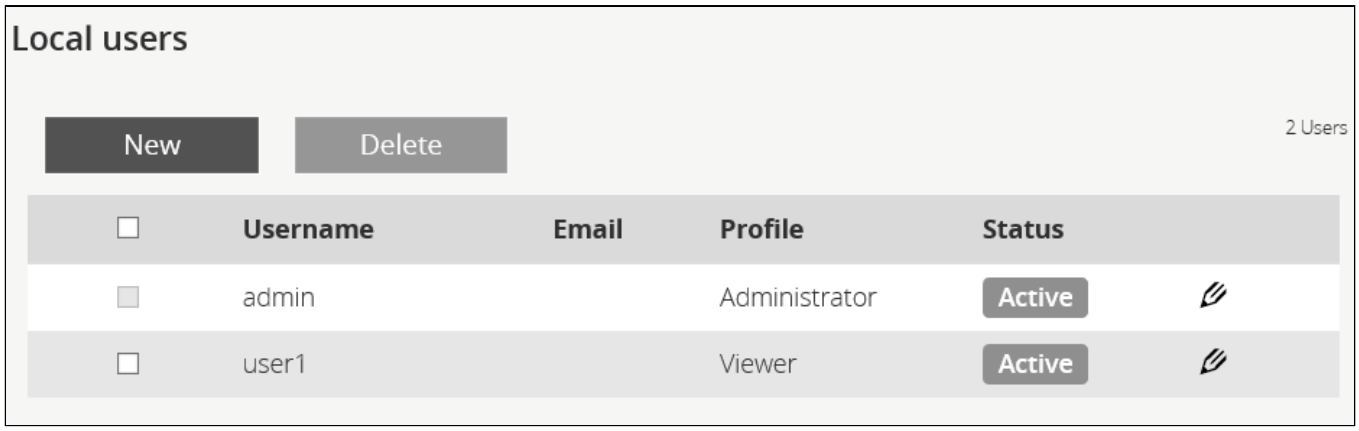
  If there is no activity, session expires after the specified amount of time.

- Session lease time (in minutes).

  If there is activity, session still expires after the specified amount of time.

Press **Save** after modifications.

Local users table



The table shows all the supported local user accounts and includes the following details:

- **Username**
- **Email**
- **Profile**

	Administrator	Operator	Viewer
Home	✓	✓	✓
Alarms	✓	✓	✓ Alarm list ✓ Export ✗ Clear
Settings	✓	✗ General ✗ Date & Time ✗ Users ✗ Network ✗ Protocols ✗ SNMP ✗ Certificates ✗ Email ✓ My preferences	✗ General ✗ Date & Time ✗ Users ✗ Network ✗ Protocols ✗ SNMP ✗ Certificates ✗ Email ✓ My preferences
Meters	✓	✓	✓ Power ✓ Battery ✓ Measure logs ✗ Configuration
Controls	✓	✓	✗
Protection	✓	✓	✗

Sensors	✅	✅	✅ Status ❌ Alarm configuration ✅ Information
Card	✅	✅ System information ❌ System logs ❌ Administration ✅ Commissioning (Sensors)	✅ System information ❌ System logs ❌ Administration ❌ Commissioning (Sensors)
Legal information (footer)	✅	✅	✅
Contextual and Full documentation	✅	✅	✅
Command Line Interface	✅	✅ get release info ✅ history ❌ ldap-test ✅ logout ❌ maintenance ❌ modbus_message_display* ❌ modbus_statistics* ✅ netconf (read-only) ❌ ping and ping6 ❌ reboot ❌ save_configuration | restore_configuration ❌ sanitize ❌ ssh-keygen ✅ time (read-only) ❌ traceroute and traceroute6 ✅ whoami	✅ get release info ✅ history ❌ ldap-test ✅ logout ❌ maintenance ❌ modbus_message_display* ❌ modbus_statistics* ✅ netconf (read-only) ❌ ping and ping6 ❌ reboot ❌ save_configuration | restore_configuration ❌ sanitize ❌ ssh-keygen ✅ time (read-only) ❌ traceroute and traceroute6 ✅ whoami

**for INDGW-M2 only*

- **Status –** Status could take following values – Inactive/Locked/Password expired/Active

Actions

Add
Press the **New** button to create up to ten new users.

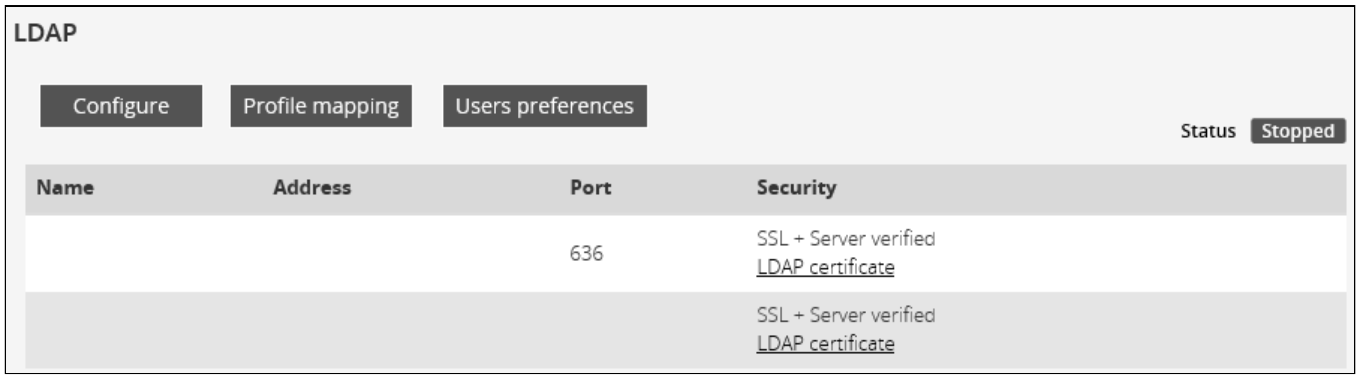
Remove
Select a user and press the **Delete** button to remove it.

Edit
Press the pen logo to edit user information and access to the following settings:

- Active
- Profile
- Username
- Full name
- Email
- Phone
- Organization – Notify by email about account modification/Password
- Reset password

- Generate randomly
- Enter manually
- Force password to be changed on next login

LDAP

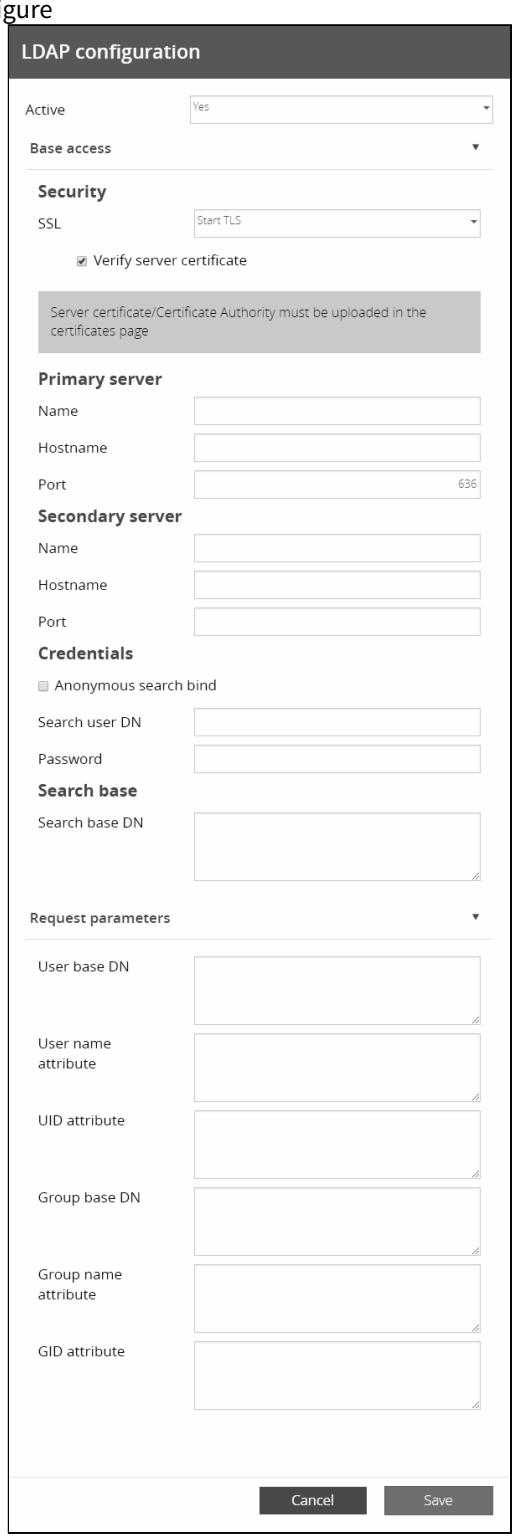


The table shows all the supported severs and includes the following details:

- Name
- Address
- Port
- Security
- Status – Status could take following values – Unreachable/Active

Actions

Configure



1. Press **Configure** to access the following LDAP settings:

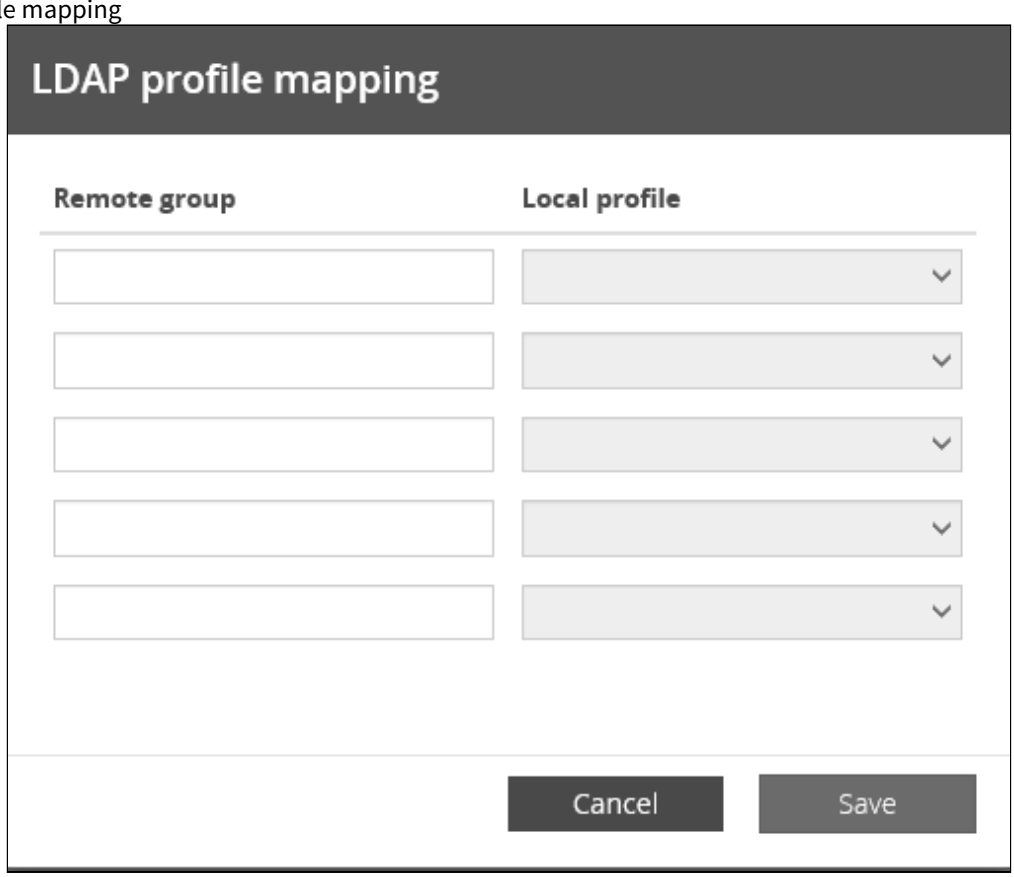
- Active
- Base access
    - Security
      SSL – None/Start TLS/SSL
      Verify server certificate
    - Primary server – Name/Hostname/Port

- Secondary server – Name/Hostname/Port
- Credentials – Anonymous search bind/Search user DN/Password
- Search base – Search base DN

- Request parameters
  - User base DN
  - User name attribute
  - UID attribute
  - Group base DN
  - Group name attribute
  - GID attribute

2. Click **Save**.

Profile mapping



1. Press **Profile mapping** to map remote groups to local profiles.
2. Click **Save**.

Users preferences

⚠ All users preferences will apply to all remote users (LDAP, RADIUS).

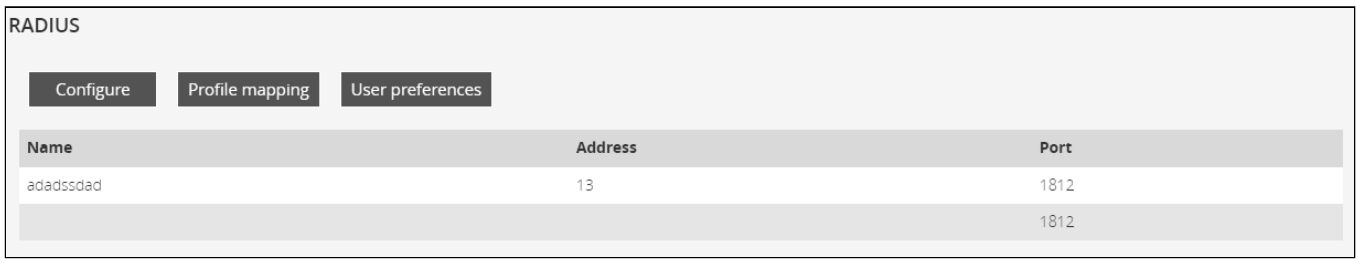
Missing screenshot

1. Press **Users preferences** to define preferences that will apply to all LDAP users
   - Language
   - Temperature
   - Date format
   - Time format

2. Click **Save**.

RADIUS

⓵ Radius is not a secured protocol, for a maximum security, it is recomended to use LDAP over TLS.

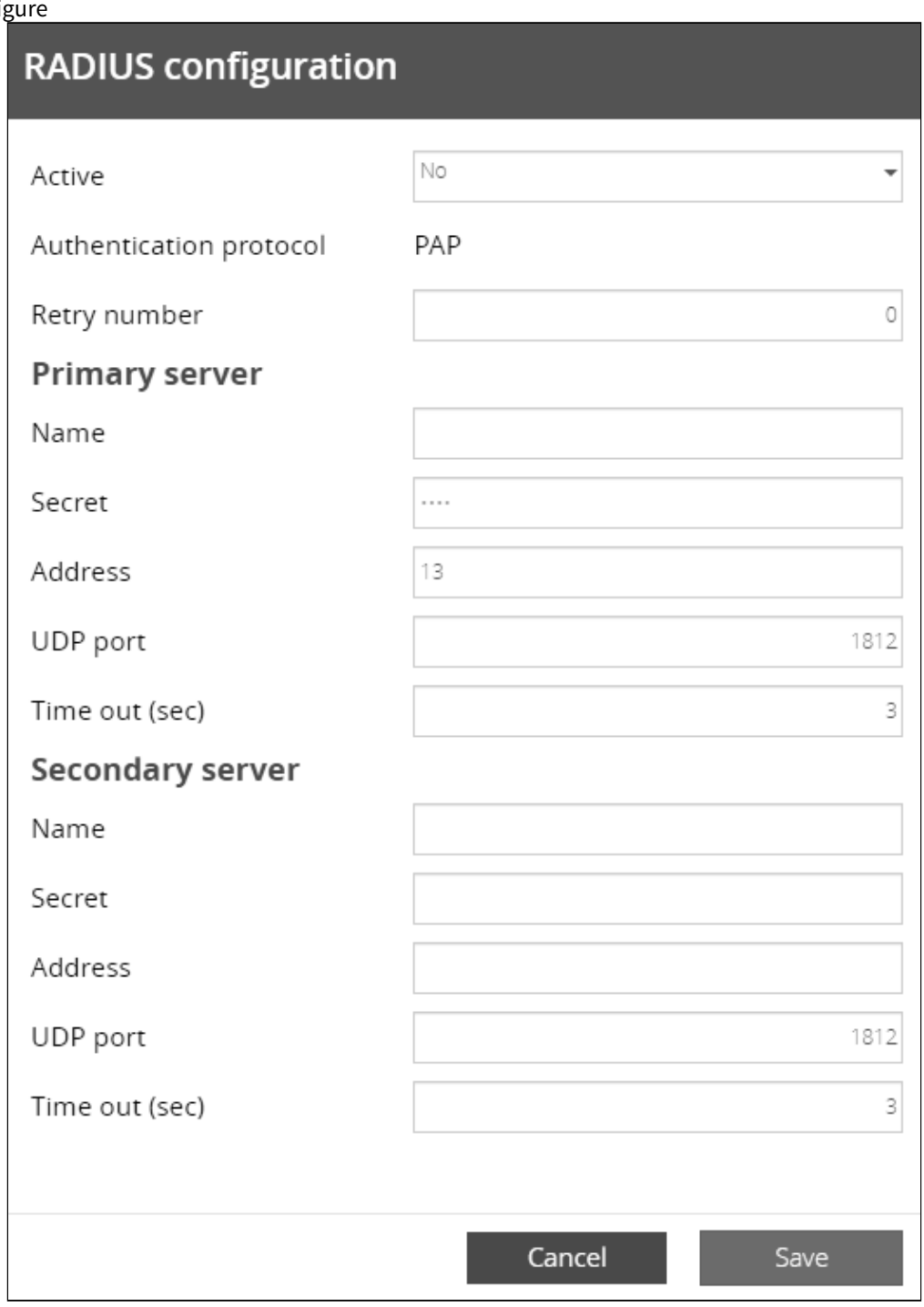


The table shows all the supported severs and includes the following details:

- Name
- Address

Actions

Configure

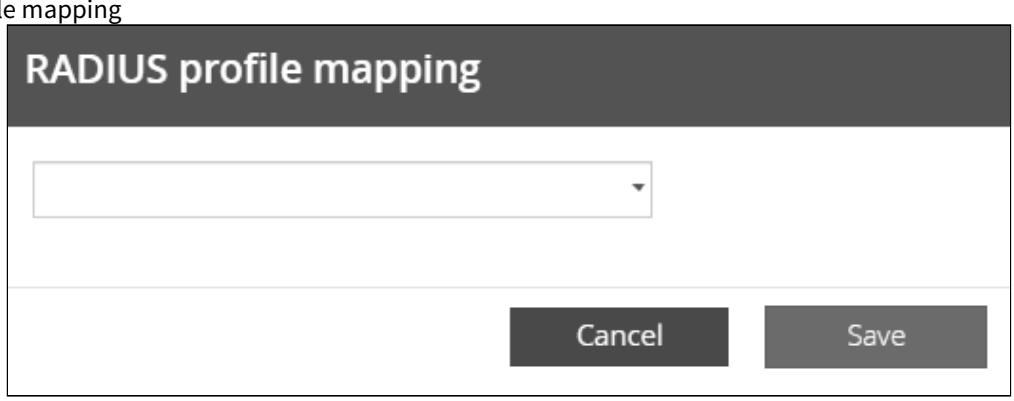


1. Press **Configure** to access the following RADIUS settings:

- Active
- Retry number
- Primary server – Name/Secret/Address//UDP port/Time out (s)
- Secondary server – Name/Secret/Address/UDP port/Time out (s)

2. Click **Save**.

Profile mapping

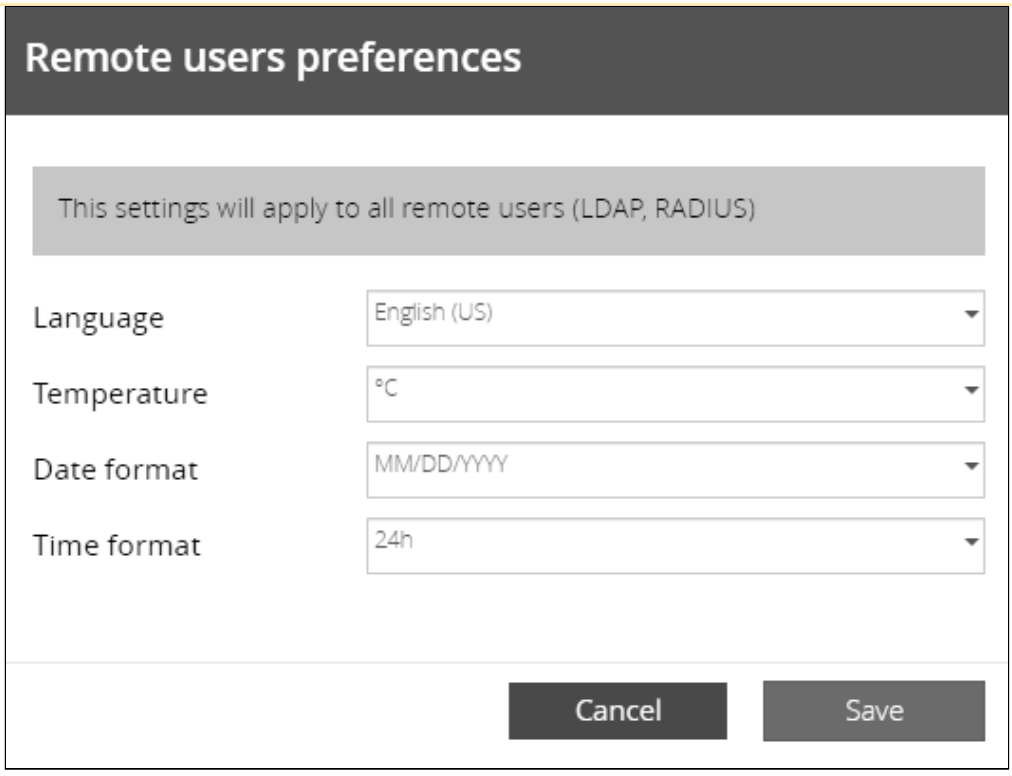


1. Press **Profile mapping** to map RADIUS profile to local profiles.

2. Click **Save**.

Users preferences

⚠ All users preferences will apply to all remote users (LDAP, RADIUS).



1. Press **Users preferences** to define preferences that will apply to all LDAP users

- Language
- Temperature
- Date format
- Time format

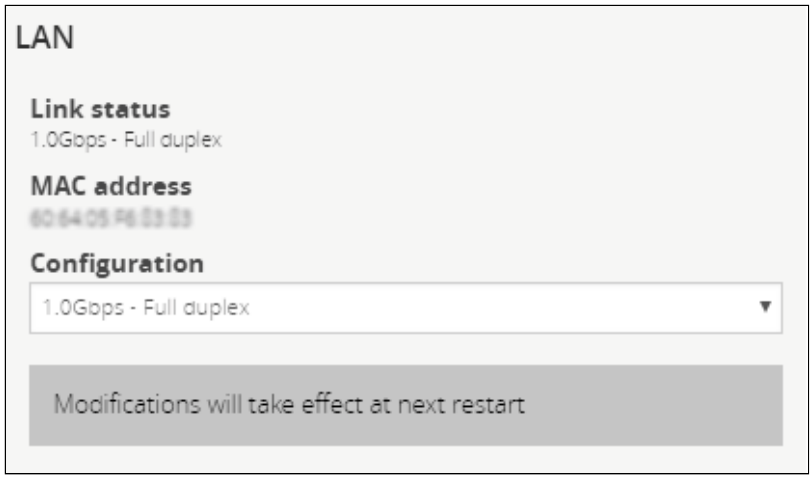
2. Click **Save**.

Default settings parameters and limitations

ⓘ For details on default parameters and limitations, see the ***Information>>>Default settings parameters*** section.

2.4.4 Network

LAN



A LAN is a computer network that interconnects computers within a limited area.

The available values for LAN configuration are listed below:

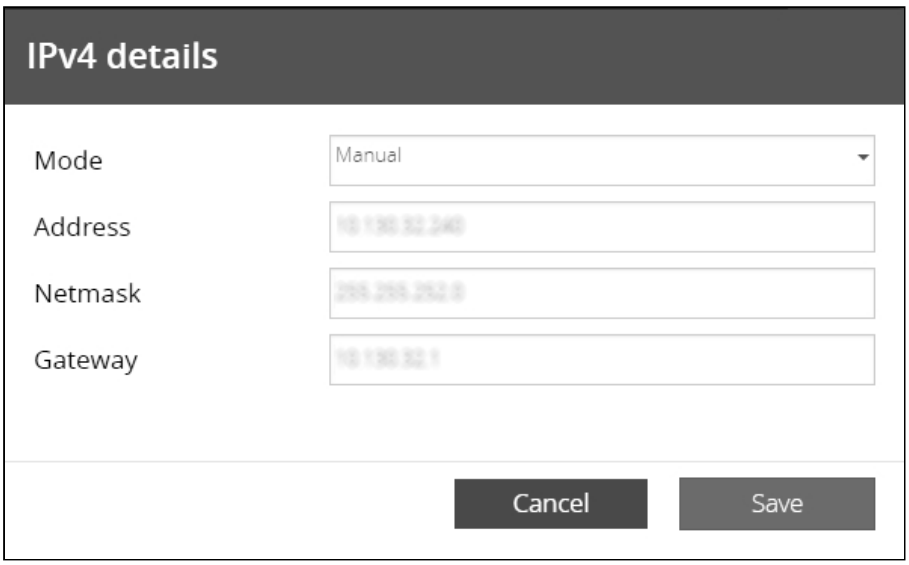
- Auto negotiation
- 10Mbps - Half duplex
- 10Mbps - Full duplex
- 100Mbps - Half duplex
- 100Mbps - Full duplex
- 1.0 Gbps - Full duplex

Any modifications are applied after the next Network Module reboot.

IPv4

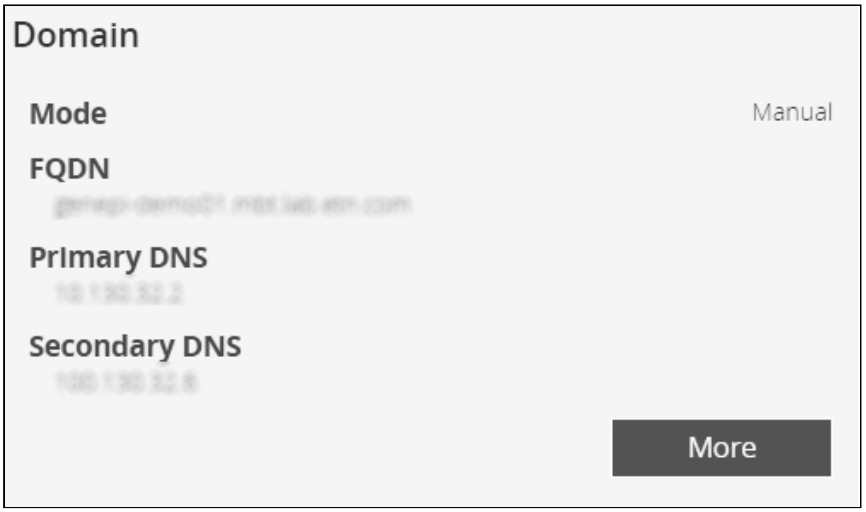
Any modifications are applied after the Network Module reboots.

Press the **More** button to configure the network settings, select either the Manual or Dynamic settings option:

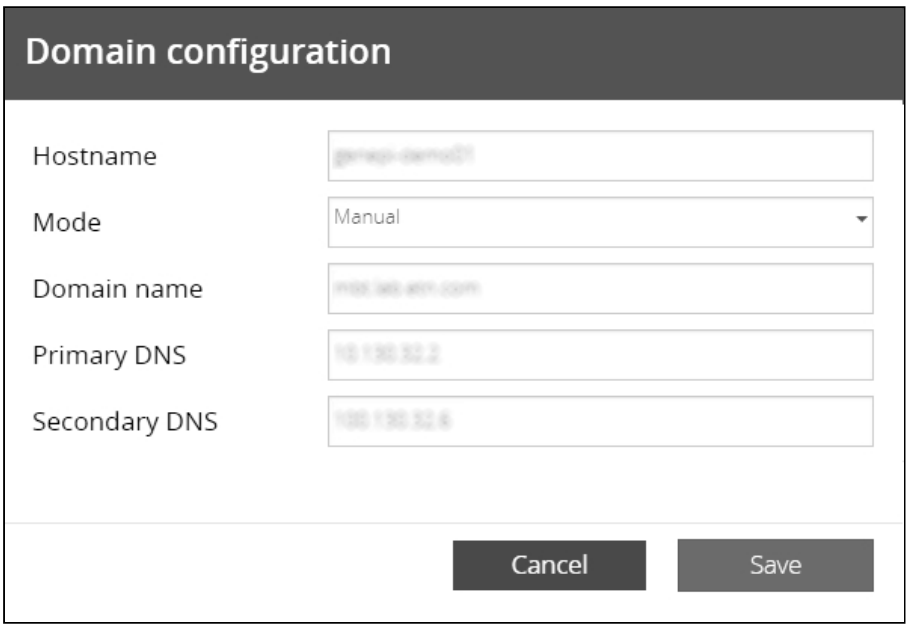


- Manual
  Select Manual, and then enter the network settings if the network is not configured with a BootP or DHCP server.
  - Enter the IP Address.
    The Network Module must have a unique IP address for use on a TCP/IP network.
  - Enter the netmask.
    The netmask identifies the class of the sub-network the Network Module is connected to.
  - Enter the gateway address.
    The gateway address allows connections to devices or hosts attached to different network segments.
- Dynamic (DHCP)
  Select dynamic DHCP to configure network parameters by a BootP or DHCP server.
  If a response is not received from the server, the UPS Network Module boots with the last saved parameters from the most recent power up. After each power up, the UPS Network Module makes five attempts to recover the network parameters.

Domain



The DNS is a hierarchical decentralized naming system for computers, services, or other resources connected to the Internet or a private network.
Press the **More** button to configure the network settings, select either the Static or Dynamic settings.



- Static
  - Enter the Network Module Hostname.
  - Enter the Network Module Domain name.
  - Primary DNS server.
    Enter the IP address of the DNS server that provides the translation of the domain name to the IP address.
  - Secondary DNS server.
    Enter the IP address of the secondary DNS server that provides the translation of the domain name to the IP address when the primary DNS server is not available.
- Dynamic
  - Enter the Network Module Hostname.

IPv6

IPV6 status and the first three addresses are displayed.
Press the **More** button to configure the network settings and get more information, press the **More** button for access to the following IPV6 details.

- Current configuration
  - Address
  - Gateway
- Address settings
  - Mode
    - Manual
      - Addresses
      - Prefix
      - Gateway
    - Router
- DNS settings
  - Get automatically (will hide the following settings)
  - Primary DNS
  - Secondary DNS

Default settings parameters and limitations

For details on default parameters and limitations, see the ***Information>>>Default settings parameters*** section.

2.4.5 Protocols

This tab contains settings for communication protocols used to get information from the device through the network, such as https for web browser.

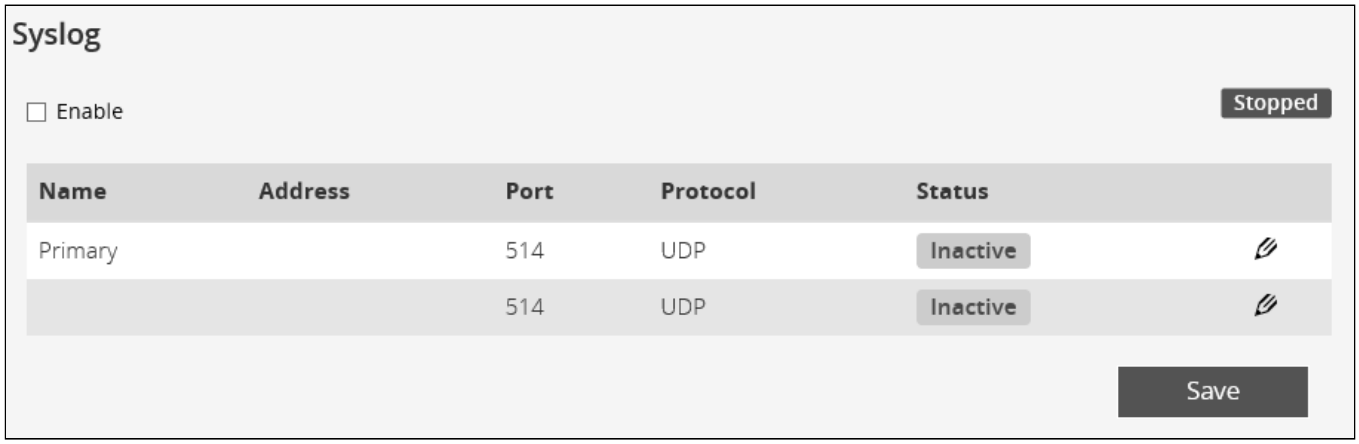
HTTPS

Only https is available.
The default network port for https is 443. For additional security, the ports can be changed on this page.

Press **Save** after modifications.

Since only https is available, port 80 is not supported.

Syslog



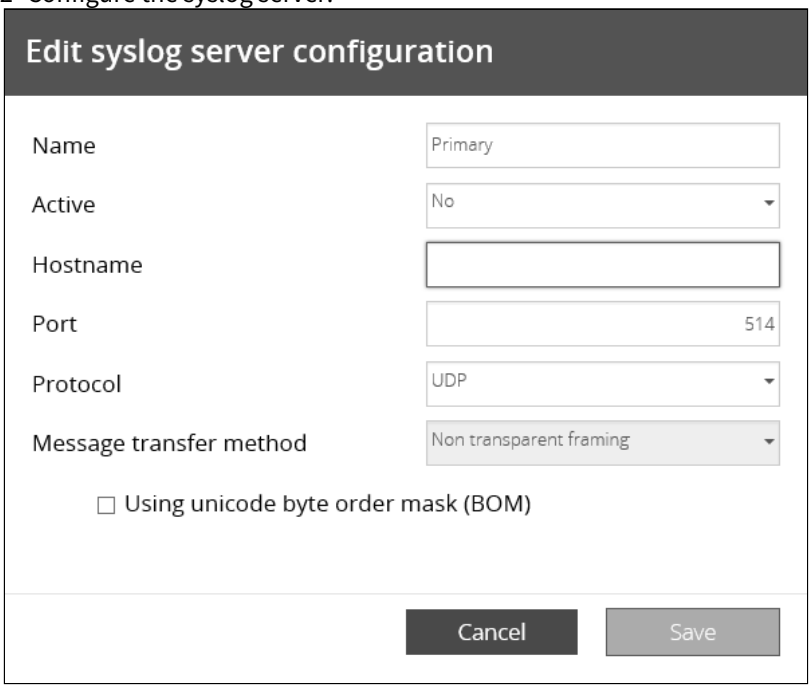
Settings

This screen allows an administrator to configure up to two syslog servers.

To configure the syslog server settings:

1- Enable syslog.
Press **Save** after modifications.

2- Configure the syslog server:



1. Click the edit icon

to access settings.

2. Enter or change the server name.
3. Select **Yes** in the Active drop-down list to activate the server.
4. Enter the Hostname and Port.
5. Select the Protocol – UDP/TCP.
6. In TCP, select the message transfer method – Octet counting/Non-transparent framing.
7. Select the option Using Unicode BOM if needed.
8. Press **Save** after modifications.

Default settings parameters and limitations

For details on default parameters and limitations, see the ***Information>>>Default settings parameters*** section.

2.4.6 SNMP

This tab contains settings for SNMP protocols used for network management systems.

Changes to authentication settings need to be confirmed by entering a valid password for the active user account.

SNMP tables

The default port for SNMP is 161 and normally this should not be changed. Some organizations prefer to use non-standard ports due to cybersecurity, and this field allows that.

SNMP monitoring Battery status, power status, events, and traps are monitored using third-party SNMP managers.

To query SNMP data, you do not need to add SNMP Managers to the Notified Application page.

To set-up SNMP managers:

1. Configure the IP address.
2. Select SNMP V1 or V1 and V3.
3. Compile the MIB you selected to be monitored by the SNMP manager.

For a list of supported MIBs, see the ***Information>>>Specifications/Technical characteristics*** section.

Press the **Supported MIBs** button to download the MIBs.

Settings

This screen allows an administrator to configure SNMP settings for computers that use the MIB to request information from the UPS Network Module.

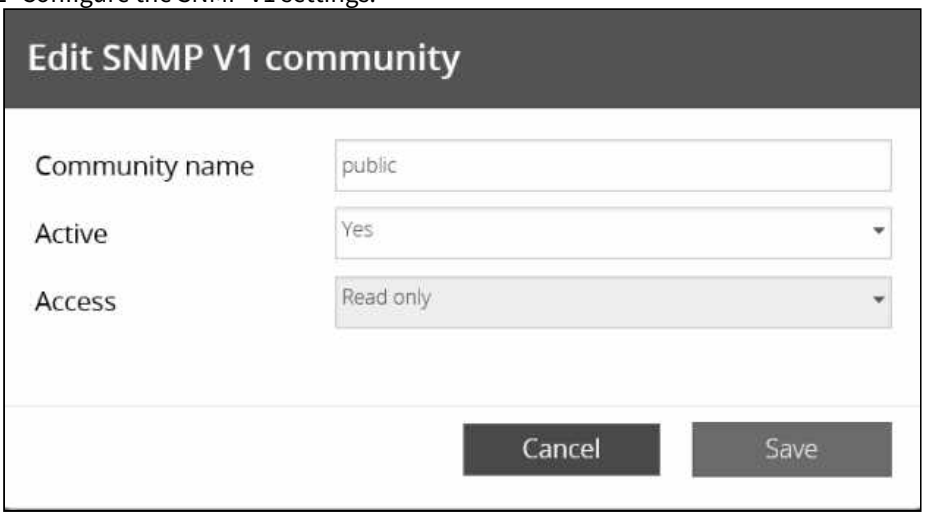
Default ports for SNMP are 161 (SNMP v1 and v3, set/get) and 162 (traps). These ports can be changed on the settings screen for additional security.

To configure the SNMP settings:

1- Enable the SNMP agent.
In addition to this also v1 and/or v3 must be enabled, along with appropriate communities and activated user accounts to allow SNMP communication.

Press **Save** after modifications.

2- Configure the SNMP V1 settings:



1. Click the edit icon

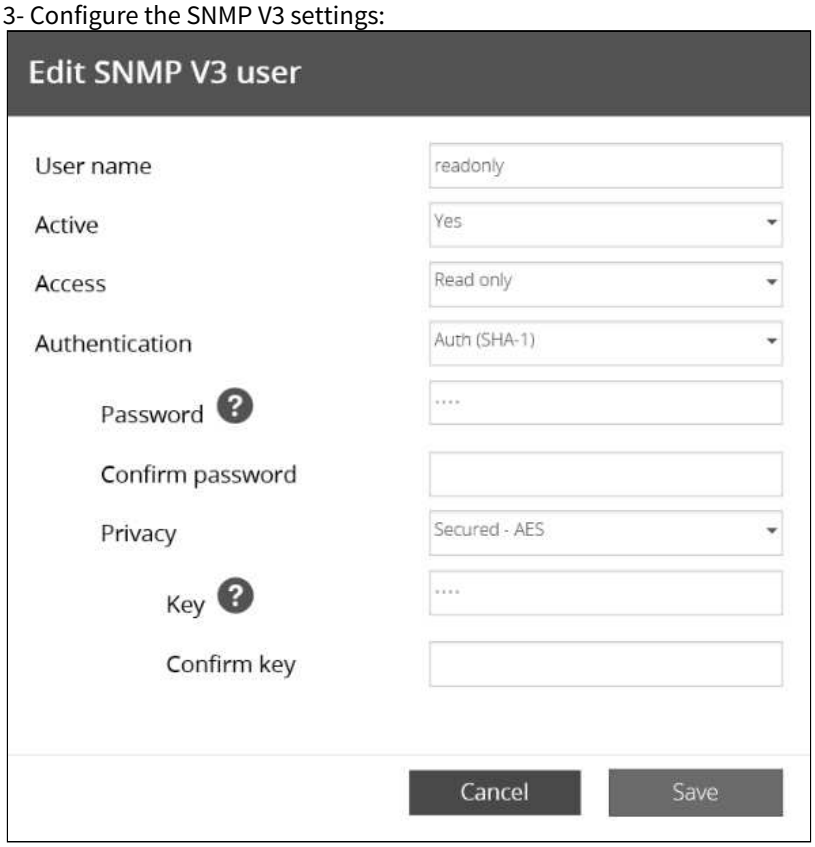
on either Read-only or Read/Write account to access settings.

2. Enter the SNMP Community Read-Only string. The UPS Network Module and the clients must share the same community name to communicate.

3. Select **Yes** in the Active drop-down list to activate the account.

4. Access level is set to display information only.

3- Configure the SNMP V3 settings:



1. Click the edit icon

on either Read Only or Read/Write account to access settings.

2. Edit the user name.
3. Select **Yes** in the Active drop-down list to activate the account.
4. Select access level.

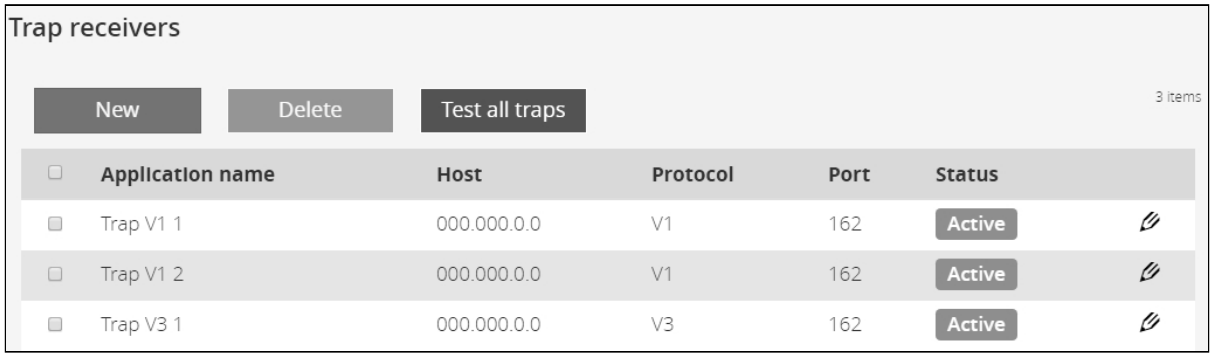
   Read only—The user does not use authentication and privacy to access SNMP variables.

   Read/Write—The user must use authentication, but not privacy, to access SNMP variables.
5. Select Authentication level.

   None— no further information is needed.

   SHA-1— fill in password and privacy keys. The password can be between 8 and 24 characters and use a combination of alphanumeric and the following special characters <>&@#%_=:;,./?|$*
6. Click **Save**.

Trap receivers

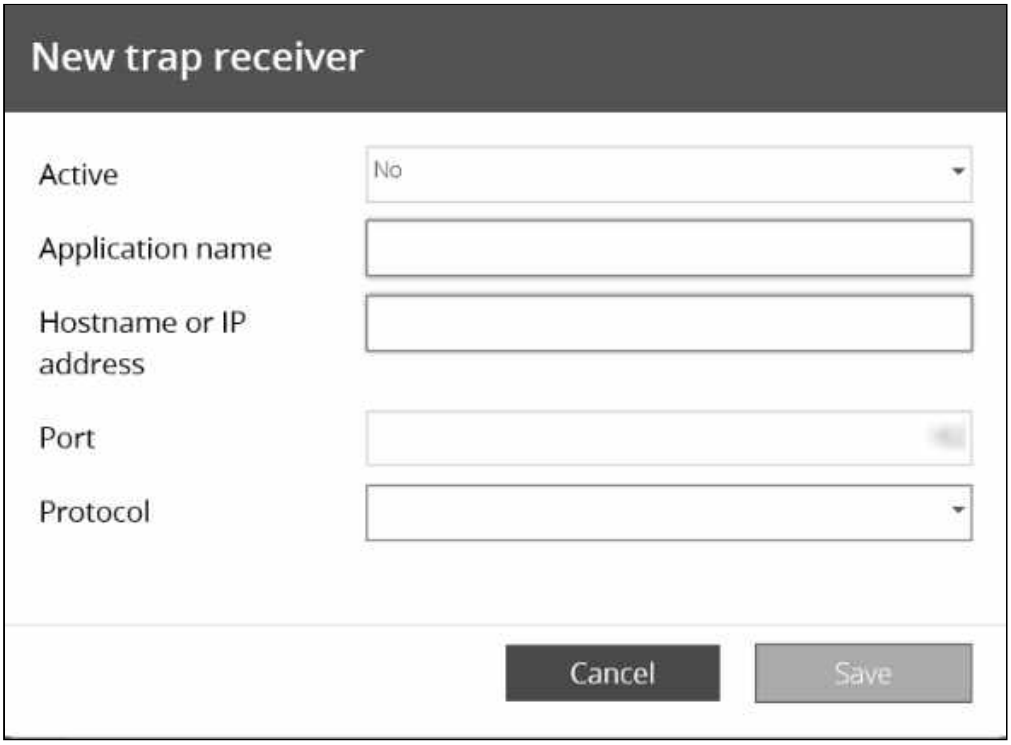


The table shows all the trap receivers and includes the following details:

- **Application name**
- **Host**
- **Protocol**
- **Port**
- **Status:** Active/Inactive/Error(configuration error)

Actions

Add



1. Press the **New** button to create new trap receivers.

2. Set following settings:

- Active – Yes/No
- Application name
- Hostname or IP address
- Port
- Protocol – V1/V3
- Trap community (V1) / User (V3)

3. Press the **SAVE** button.

Remove

Select a trap receiver and press the **Delete** button to remove it.

Edit

Press the pen icon to edit trap receiver information and access to its settings.

Test all traps

Press the **Test all traps** button to send the trap test to all trap receivers.

Separate window provides the test status with following values:

- In progress
- Request successfully sent
- invalid type

For details on SNMP trap codes, see the ***Information>>>SNMP traps*** section.

Default settings parameters and limitations

For details on default parameters and limitations, see the ***Information>>>Default settings parameters*** section.

2.4.7 Certificates

Local certificates

Manage local certificates by :

- Generating CSR and import certificates signed by the CA.
- Generating new self-signed certificates.

Local certificates table

The table shows the following information for each local certificate.

- Used for
- Issued by
- Valid from
- Expiration
- Status — valid, expires soon, or expired

Actions

Revoke
This action will take the selected certificate out of use.

Select the certificate to revoke, and then press the **Revoke** button.

A confirmation window appears, press **Continue** to proceed, this operation cannot be recovered.

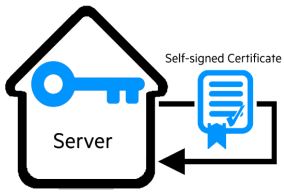
Revoke will replace current certificate by a new self-signed certificate.
This may disconnect connected applications:
- Web browsers
- Shutdown application
- Monitoring application
The certificate that is taken out of use with the revoke action cannot be recovered.

Export
Exports the selected certificate on your OS browser window.

Edit
Allows access to the following:

- Certificate summary
- Actions
  Generate a new self-signed certificate.
  Generate CSR.
  Import certificate (only available when CSR is generated).
- Details

Generate a new self-signed certificate



To replace a selected certificate with a new self-signed certificate.

This may disconnect applications such as a Web browser, shutdown application, or monitoring application.

This operation cannot be recovered.

Create new certificates:

CSR

Press **Generate Signing Request** button in the in the certificate edition.

The CSR is automatically downloaded.

CSR must be signed with the CA, which is managed outside the card.

Import certificate

When the CSR is signed by the CA, it can be imported into the Network Module.

When the import is complete, the new local certificate information is displayed in the table.

Certificate authorities (CA)

Manages CAs.

CA table

The table displays certificate authorities with the following details:

- Used for
- Issued by
- Issued to
- Valid from
- Expiration
- Status — valid, expires soon, or expired

Actions

Import
When importing the CA, you must select the associated service, and then upload process can begin through the OS browser window.

Revoke
Select the certificate to revoke, and then press the **Revoke** button.

A confirmation window appears, press **Continue** to proceed, this operation cannot be recovered.

Export
Exports the selected certificate on your OS browser window.

Edit
Gives access to a summary of the certificate.

Pairing with clients

For details on pairing instructions, follow the link **pairing instructions** in the tile or see the **Servicing the Network Management Module*>>>Pairing agent to the Network Module*** section.

During the selected timeframe, new connections to the Network Module are automatically trusted and accepted.

After automatic acceptance, make sure that all listed clients belong to your infrastructure. If not, access may be revoked using the Delete button.

The use of this automatic acceptance should be restricted to a secured and trusted network.

For maximum security, we recommend following one of the two methods on the certificate settings page:

- Import agent's certificates manually.

- Generate trusted certificate for both agents and Network Module using your own PKI.

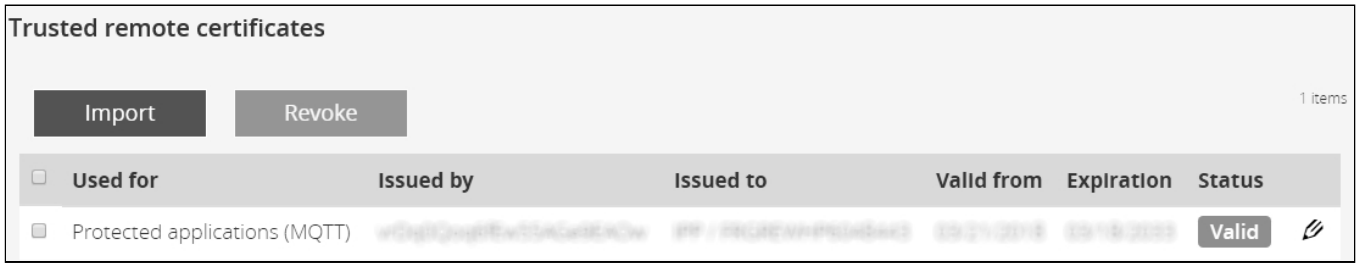
Actions

Start
Starts the pairing window during the selected timeframe or until it is stopped.

Time countdown is displayed.

Stop
Stops the pairing window.

Trusted remote certificates



The table shows the following information for each trusted remote certificate.

- Used for
- Issued by
- Issued to

- Valid from
- Expiration
  In case a certificate expires, the connection with the client will be lost. If this happens, the user will have to recreate the connection and associated certificates.
- Status — valid, expires soon, or expired

Actions

Import
When importing the client certificate, you must select the associated service, and then upload process can begin through the OS browser window.

Revoke
Select the certificate to revoke, and then press the **Revoke** button.

A confirmation window appears, press **Continue** to proceed, this operation cannot be recovered.

Edit
Gives access to a summary of the certificate.

2.4.8 Email

Email sending configuration

For examples on email sending configuration see the **Servicing the Network Management Module>>>Subscribing to a set of alarms for email notification** section.

Email sending configuration table

The table shows all the email sending configuration and includes the following details:

- **Configuration name**
- **Email address**
- **Configuration**
  Configuration displays Email delegation/Events notification/Periodic report icons when active.
- **Status** – Active/Inactive/In delegation

Actions

Add
Press the **New** button to create a new email sending configuration.

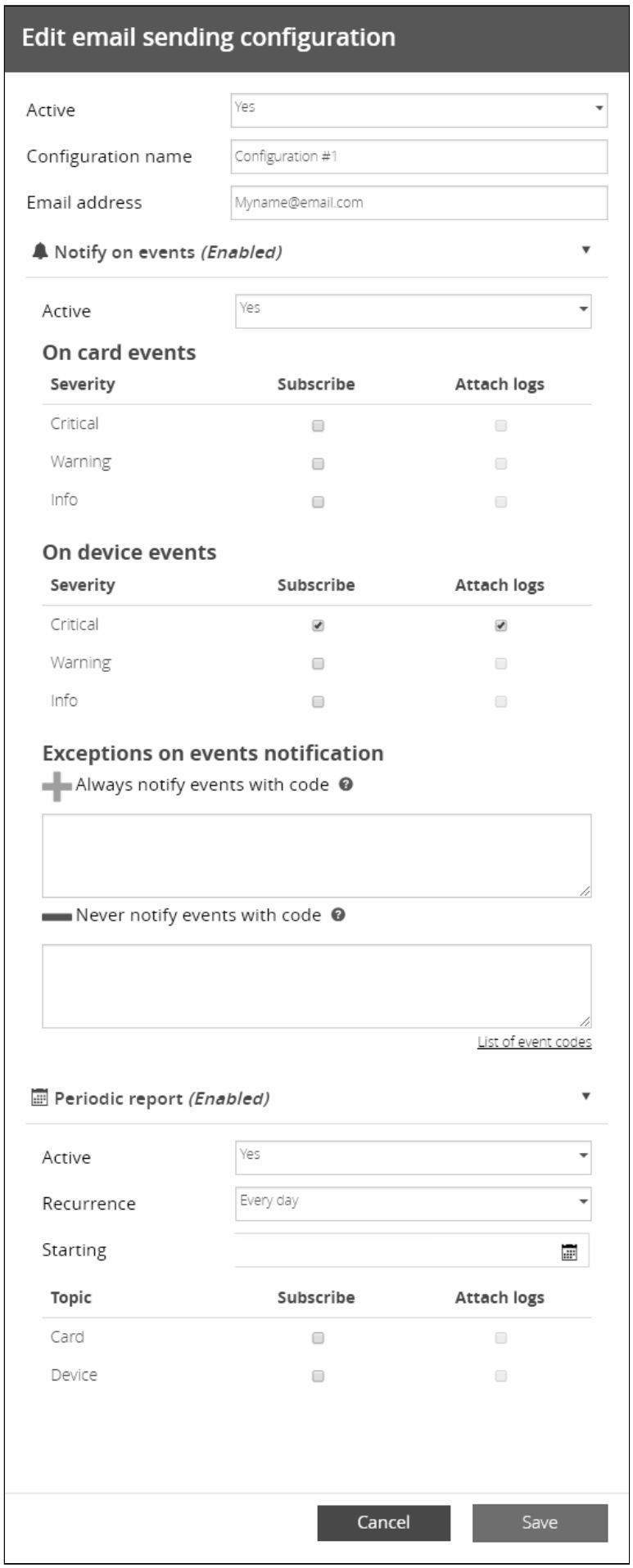
Remove
Select an email sending configuration and press the **Delete** button to remove it.

Edit

Press the pen icon to edit email sending configuration and access to the following settings:

- Active

- Configuration name
- Email address
- Notify on events – Severity level/Attach logs/Exceptions on events notification
- Periodic report – Active/Recurrence/Starting/Topic selection – Card/Devices


Edit email sending configuration
Active
Yes
Configuration name
Configuration #1
Email address
Myname@email.com
Notify on events (Enabled)
Active
Yes
On card events
Severity
Subscribe
Attach logs
Critical
Warning
Info
On device events
Severity
Subscribe
Attach logs
Critical
Warning
Info
Exceptions on events notification
Always notify events with code
Never notify events with code
List of event codes
Periodic report (Enabled)
Active
Yes
Recurrence
Every day
Starting
Topic
Subscribe
Attach logs
Card
Device
Cancel
Save

SMTP

SMTP is an internet standard for electronic email transmission.

The following SMTP settings are configurable:

- Server IP/Hostname – Enter the host name or IP address of the SMTP server used to transfer email messages in the SMTP Server field.
- Port
- Sender address
- Secure SMTP connection
- Verify certificate authority
- SMTP server authentication

Select the SMTP server authentication checkbox to require a user name and a password for SNMP authentication.

Enter the Username and the Password.

- Save and test server configuration

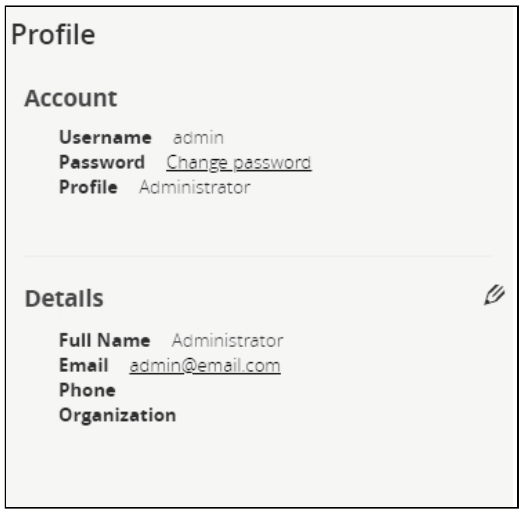
Default settings parameters and limitations

For details on default parameters and limitations, see the ***Information>>>Default settings parameters*** section.

2.4.9 My preferences

This page is in read-only mode when connected through LDAP and it displays the preferences applied to all LDAP users as configured in the ***Settings>>>Users>>>LDAP-Users preferences*** section.

Profile



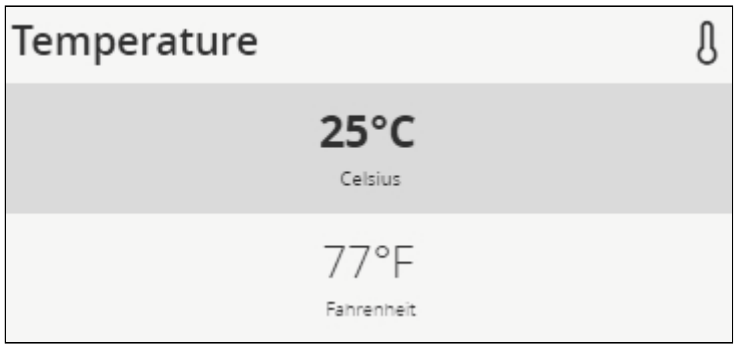
Click on **Change password** to change the password.

> ⚠ In some cases, it is not possible to change the password if it has already been changed within a day period. Refer to the troubleshooting section.

If you have the administrator's rights, you can press the **pen logo** to edit user profile and update the following information:

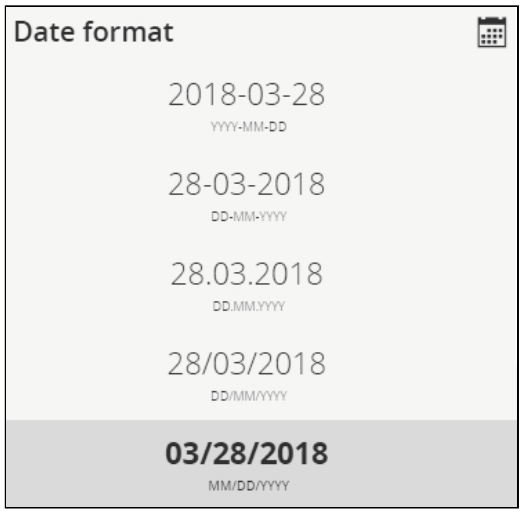
- Full name
- Email
- Phone
- Organization

Temperature



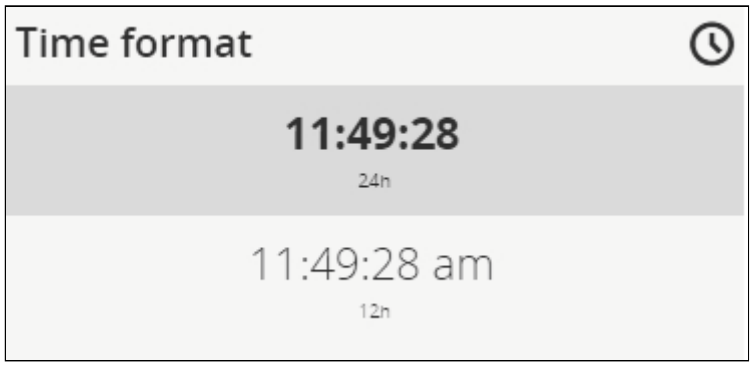
- °C (Celsius)
- °F (Fahrenheit)

Date format



- YYYY-MM-DD
- DD-MM-YYYY
- DD.MM.YYYY
- DD/MM/YYYY
- MM/DD/YYYY
- DD MM YYYY

Time format



- hh:mm:ss (24h)
- hh:mm:ss (12h)

Language

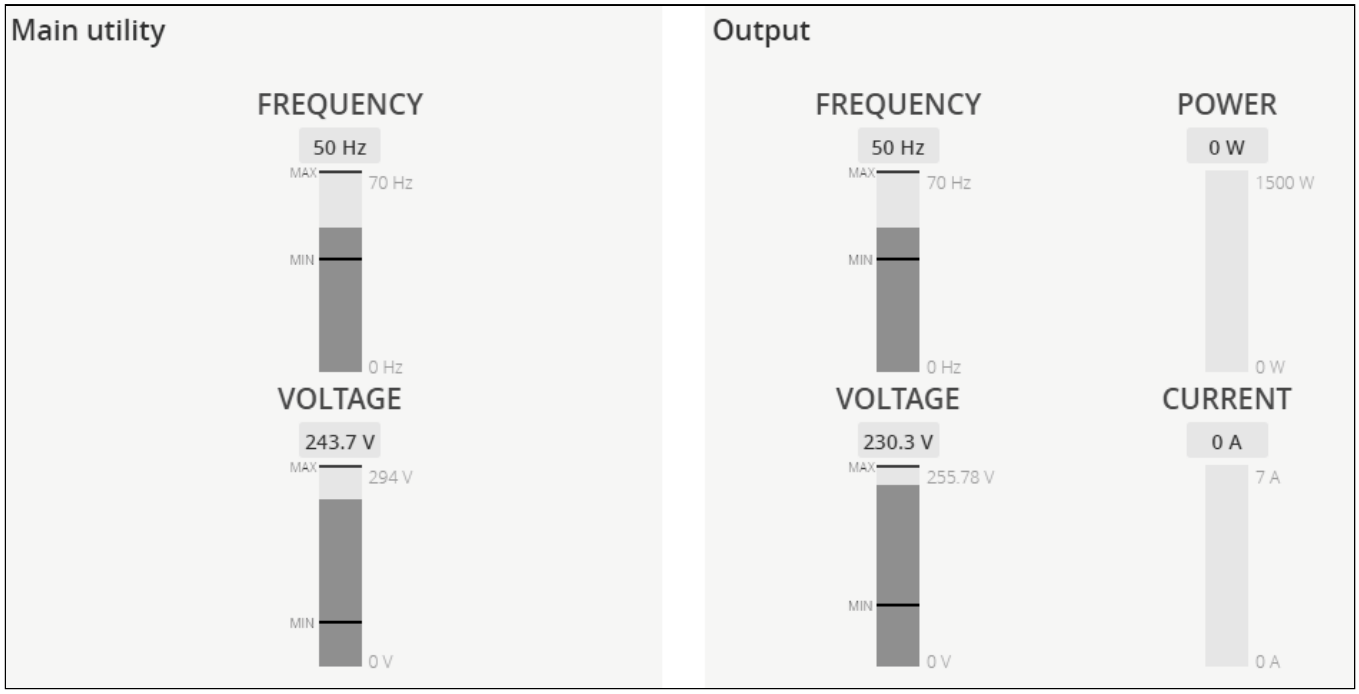
- German
- English
- Spanish
- French
- Italian
- Japanese
- Simplified Chinese
- Traditional Chinese

Default settings parameters and limitations

For details on default parameters and limitations, see the ***Information>>>Default settings parameters*** section.

2.5 Meters

2.5.1 Power



Displays the product input and output measures.

> The numbers on the right side of a gauge show the scale.
> They do not indicate allowed or observed minimum or maximum levels.

Input

- Frequency (Hz)
- Voltage (V)

Output

- Frequency (Hz)
- Voltage (V)
- Power (W)
- Current (A)

2.5.2 Battery

Battery section is an overview of the battery information and allow to launch a battery test.

> The information displayed depends on the device.

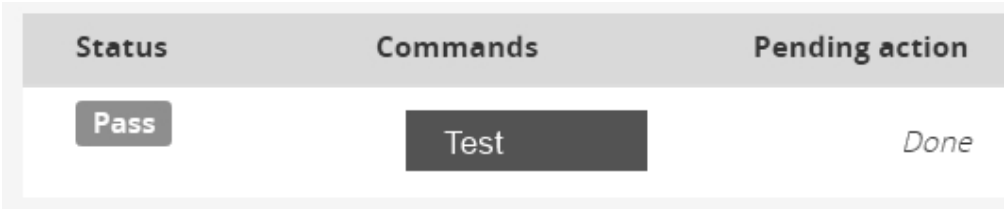
Overview

- Type
- Nominal capacity
- Nominal voltage
- Capacity remaining
- Runtime
- State
- Recommended replacement date
- State of health

Details

- Voltage
- Current
- Temperature
- Min cell voltage
- Max cell voltage
- Number of cycles
- Min temperature
- Max temperature
- BMS state

Test



Status

Battery test status reflects the last completed battery test result, as well as its critical status (color) and completion time.

- Pass
- Warning
- Fail
- Unknown

Commands

Start button is disabled if a battery test is already in progress or scheduled.

The Abort button is enabled only when a test is in progress or scheduled.

Pending action

The pending action reflects the battery test status**.**

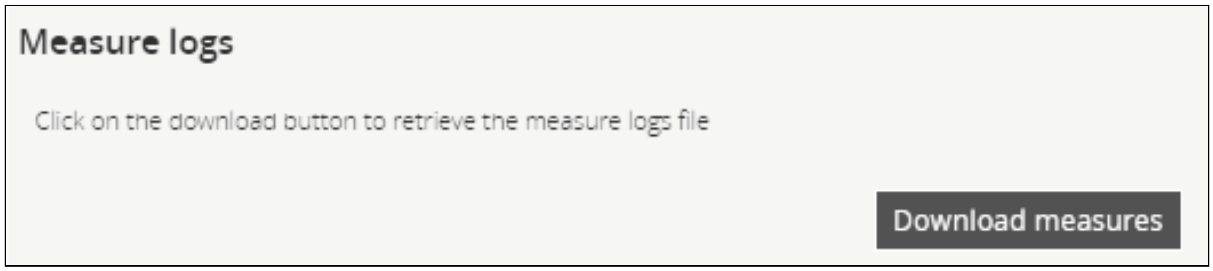
- None
- Scheduled
- In progress
- Aborted
- Done

2.5.3 Measure logs

Configuration

This log configuration allows to define the log acquisition frequency.

Measure logs



Press the **Download measures** button to download the log file.
If available, possible measures are listed below:

- Input Voltage (V)
- Input Frequency (Hz)
- Bypass Voltage (V)
- Bypass Frequency (Hz)
- Output Voltage (V)
- Output Frequency (Hz)
- Output Current (A)
- Output Apparent Power (VA)
- Output Active Power (W)
- Output Power Factor
- Output Percent Load (%)
- Battery Voltage (V)
- Battery Capacity (%)
- Battery Remaining Time (s)

Default settings parameters and limitations

For details on default parameters and limitations, see the ***Information>>>Default settings parameters*** section.

2.6 Controls

2.6.1 UPS

Entire UPS

Controls are displayed for the entire UPS, and not for specific outlet options.

The table in this section displays UPS status, the associated commands (on/off), and the pending action.

Status

Reflects the current mode of the UPS. The following is a list of potential table values that are displayed based on the UPS topology.

- On — Protected/Not protected
- Off — Not powered/Not protected

Commands

A set of commands are available and activated when one of the following buttons is pressed. A confirmation window appears.

- **Safe OFF**

This will shut off the load. Protected applications will be safely powered down.

This control is available only if the status is not OFF and if there are no active commands running.

- **Safe reboot**

This will shut off and then switch ON the load. Protected applications will be safely powered down.

This control is available only if the status is not OFF and if there are no active commands running.

- **Switch ON**

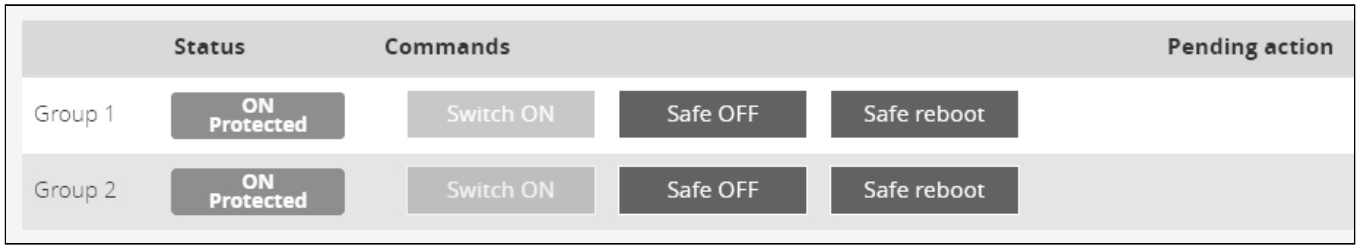
This will switch ON the load or turn ON the online UPS.

This control is available when the status is OFF, if there are no active commands running and if the Online UPS is on bypass.

Pending action

Displays the delay before shutdown and delays before startup.

2.6.2 Outlets



Group 1/ Group 2

Load segmentations allow, battery runtime to remain on essential equipment and automatically power down non-priority equipment during an extended power outage.

This feature is also used for remote reboot and the sequential start of servers to restrict inrush currents.

Status

It reflects the current outlet status.

- On — Protected/Not protected
- Off — Not powered

Commands

A set of commands are available and activated when one of the following buttons is pressed. A confirmation window appears.

- **Safe OFF**

This will shut off the load connected to the associated load segment. Protected applications are safely powered down.

This control is available only if the status is not OFF and if there are no active commands running.

- **Safe reboot**

This will power down and then switch ON the load connected to the associated load segment. Protected applications are safely powered down.

This control is available only if the status is not OFF and if there are no active commands running.

- **Switch ON**

This will switch ON the load connected to the associated load segment.

This control is available when status is OFF and if there are no active commands running.

Pending action

Displays the delay before shutdown and delay before startup.

2.7 Protection

2.7.1 Scheduled shutdowns

Use Scheduled shutdowns to turn off either the UPS or individual load segments at a specific day and time.

This feature is used for saving energy by turning off equipment outside of office hours or to enhance cybersecurity by powering down network equipment.

If server shutdown scenarios are defined for any of the connected servers or appliances, they will be triggered before the corresponding outlets are turned off as configured in shutdown settings.

Scheduled shutdowns table

The table displays the scheduled shutdowns and includes the following details.

- **Active –** Yes/No
- **Recurrence –** Once/Every day/Every week
- **Load segment –** Primary/Group 1/Group 2
- **Shutdown –** Date/Time
- **Restart –** Date/Time

Actions

New

Press the **New** button to create a scheduled shutdown.

Remove

Select a schedule shutdown and press the **Remove** button to delete the scheduled shutdown.

Edit

Press the pen icon to edit schedule shutdown and to access the settings.

2.7.2 Agent list

Pairing with shutdown agents

For details on pairing instructions, follow the link **pairing instructions** in the tile or see the **Servicing the Network Management Module*>>>Pairing agent to the Network Module*** section.

Authentication and encryption of connections between the UPS network module and shutdown agents is based on matching certificates. Automated pairing of shutdown agents and UPS network modules is recommended in case the installation is done manually in a secure and trusted network, and when certificates cannot be created in other ways.

During the selected timeframe, new agent connections to the Network Module are automatically trusted and accepted.

After automatic acceptance, make sure that all listed agents belong to your infrastructure. If not, access may be revoked using the **Delete** button.

For maximum security, Eaton recommend following one of the two methods on the **certificate settings** page:

- import client certificates manually.

- generate trusted certificate for both clients and Network Module using your own PKI.

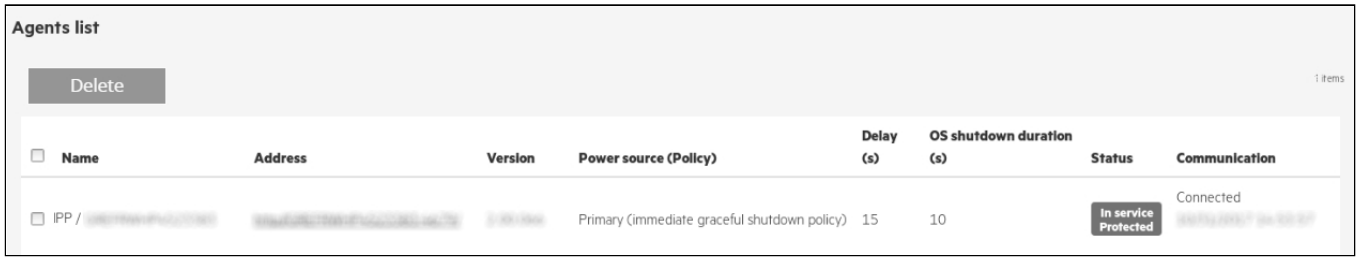
Actions

Start
Starts the pairing window for the selected timeframe or until it is stopped.

Time countdown is displayed.

Stop
Stops the pairing window.

Agent list table



The table displays the IPP agent list that is connected to the Network Module and includes the following details:

- Name
- Address
- Version of the Agent
- Power source (Policy)
- Delay (in seconds)
- OS shutdown duration (in seconds)
- Status
    - In service | Protected
    - In service | Not protected
    - Stopping | Protected
    - Stopped | Protected
- Communication
    - Connected | yyyy/mm/dd hh:mm:ss
    - Lost | yyyy/mm/dd hh:mm:ss

Actions

Delete

When the agent is connected, the Delete function will not work correctly because the agent will keep on trying to re-connect.
So connect to the software, remove the Network module from the Software nodes list (in the nodes list, right click on the Network module and click **remove nodes**).

When communication with the agent is lost, agent can be deleted by using the **Delete** button.

Select an agent and press the **Delete** button to delete the agent.

2.7.3 Agent settings

Agent shutdown sequence timing

All agents that are connected to the Network Module are displayed in tables by power sources.

- Primary
- Group 1
- Group 2

The 'local agent' setting is used for setting for example a minimum shutdown duration, or a power down delay for a load segment that has no registered shutdown agents. One use case would be a load segment that powers network equipment that needs to stay on while servers and storage perform their orderly shutdown.

The tables include the following details:

- Name
- Delay (in seconds)
- OS shutdown duration (in seconds)

Actions

Set Delay

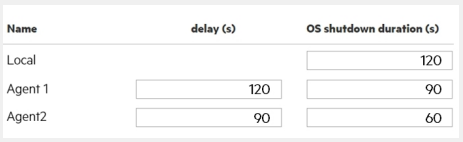
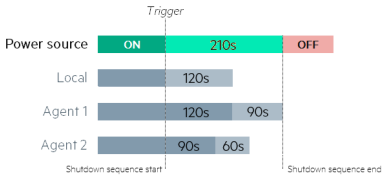
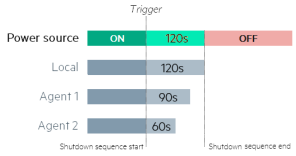
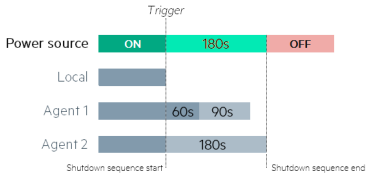
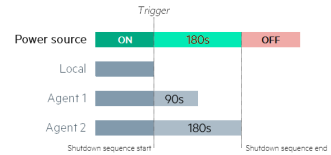
Select and directly change the setting in the table and then **Save**.

Set OS shutdown duration

Select and directly change the setting in the table and then **Save**.

Examples

Examples below show the impact of agent settings on the shutdown sequence for an ordered shutdown or an immediate shutdown.

Agent settings examples	Sequential shutdown	Immediate shutdown
		
		

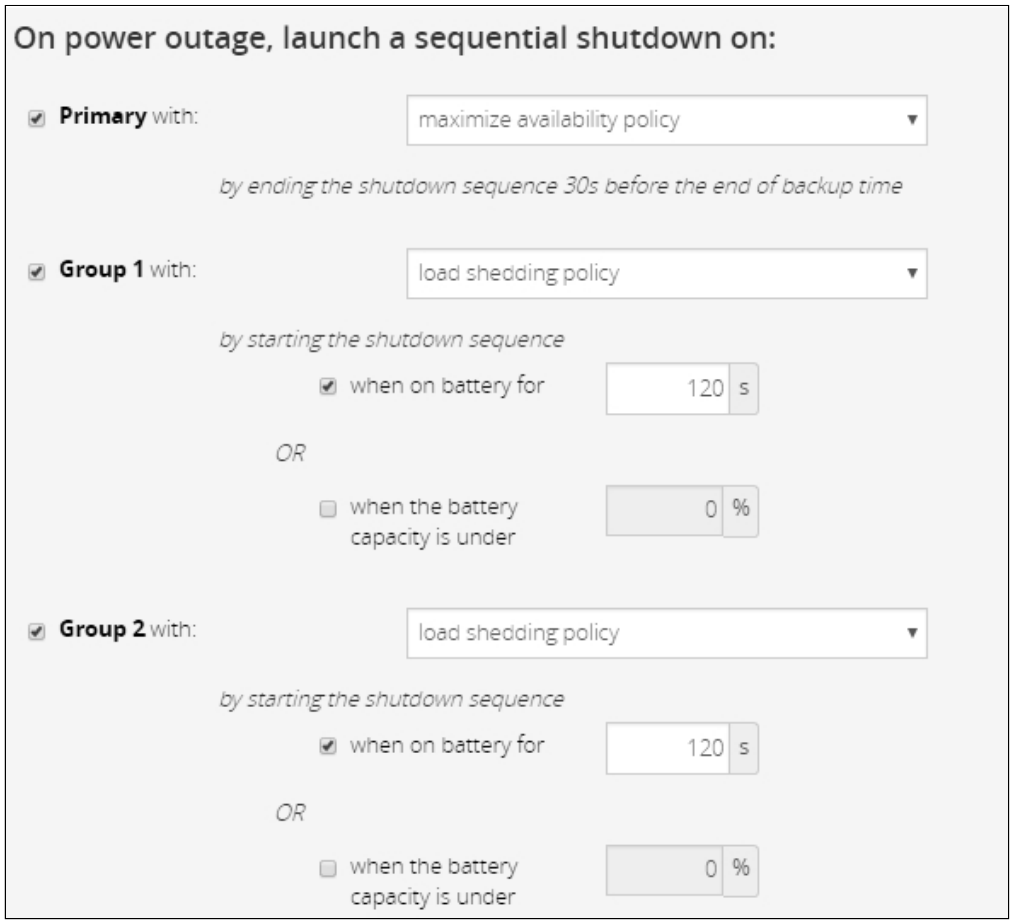
Note:
The trigger in the diagram is the moment when the shutdown sequence starts, and it is defined in the power outage policy section for each power source.

2.7.4 Power outage policy

These setting are in conjunction with the shutdown agents and control how the network module directs the shutdown of protected servers and appliances. It gives the possibility to prioritize and schedule shutdown actions so that the IT system is powered down in the correct order. For example, applications first, database servers next, and storage last. It is also possible to turn off some outlets to reduce power consumption and get longer battery runtime for the most important devices.

For examples on Powering down applications see the **Servicing the Network Management Module>>>Powering down/up applications examples** section.

On power outage



Policies are set per power source (outlet groups) if they are present in the UPS.

Enable/Disable

For each power source, the shutdown policy can be enabled or disabled with check-boxes.

When disabled, the policy will be greyed out.

Set the policy

The available policies for shutdown are listed below from preset to customized settings:

Preset policies

- Maximize availability — To end the shutdown 30s before the end of backup time.
- Immediate graceful shutdown — To start the shutdown after 30s of backup time.

Custom policies

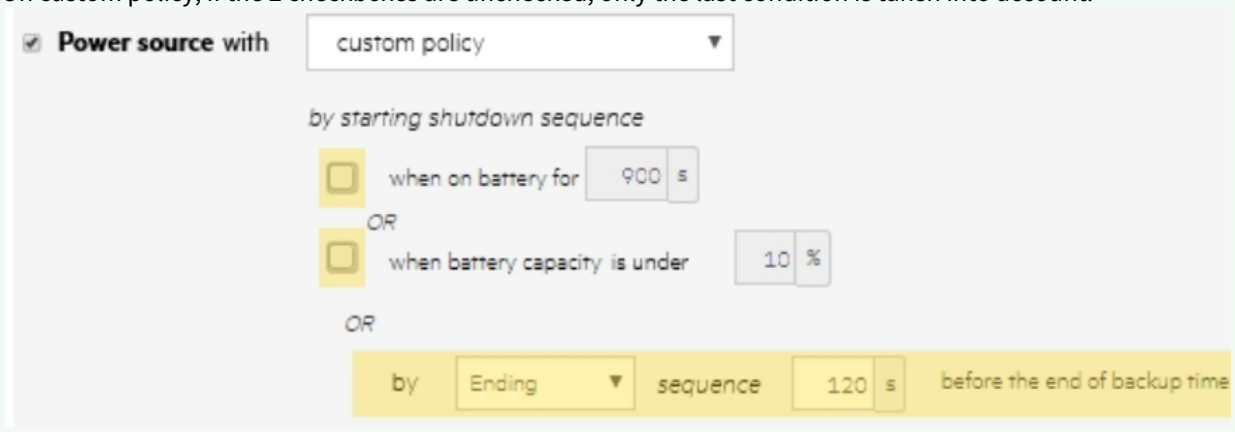
When there are several conditions to start the shutdown sequence, the shutdown sequence will start as soon as one of the conditions is reached.

- Load shedding — To start the shutdown when on battery for the set time in (s) or when battery capacity reaches the set capacity in (%). When disabled, the condition is greyed out.
- Custom — Same as load shedding but with 2 additional options:
  - to end the shutdown after the set time in (s) before the end of backup time.
  - to start shutdown after the set time in (s) before the end of backup time.

⚠ When primary shuts OFF, both group1 and group 2 shut OFF immediately.
So if Primary is set to one of the following:

- Immediate graceful shutdown — groups policies should be restricted to Immediate graceful shutdown.
- Load shedding — groups policies should avoid Maximize availability.

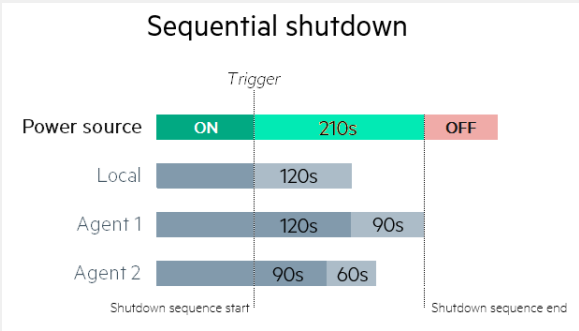
On custom policy, if the 2 checkboxes are unchecked, only the last condition is taken into account.



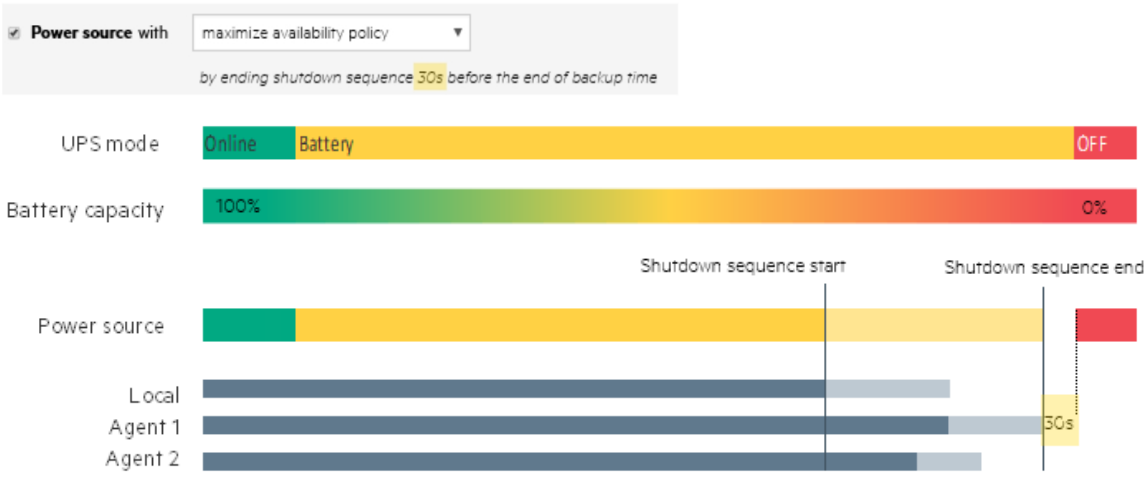
Settings examples

All the following examples are using below agent's settings.

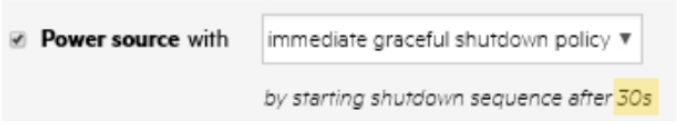
Name	delay (s)	OS shutdown duration (s)
Local		120
Agent 1	120	90
Agent2	90	60

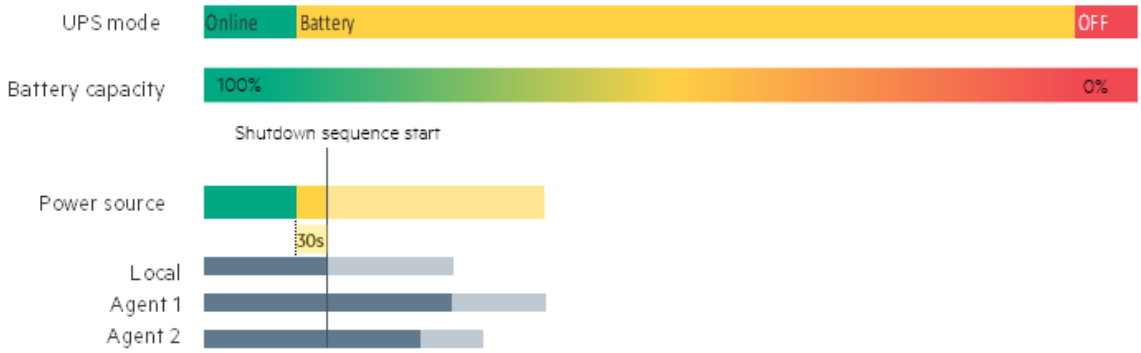


- Example 1: Maximize availability policy

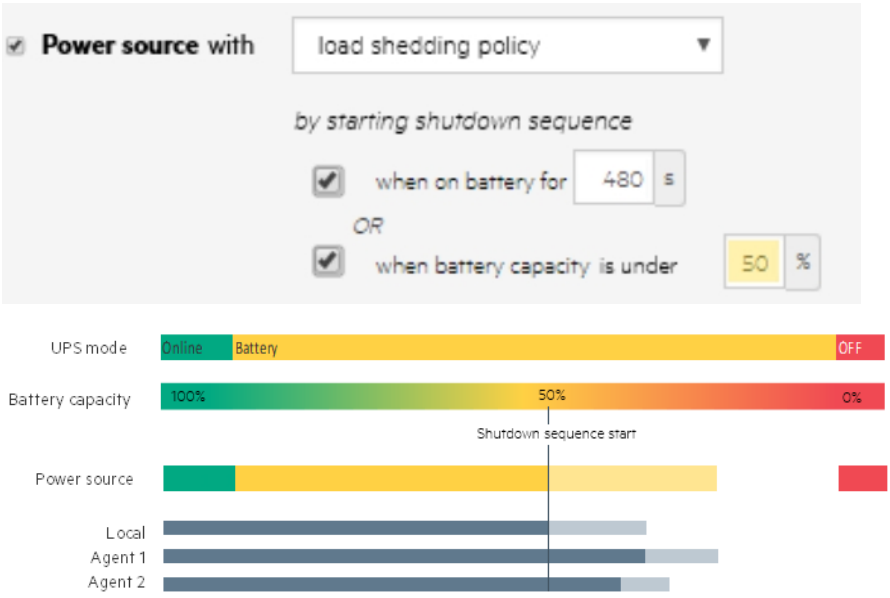
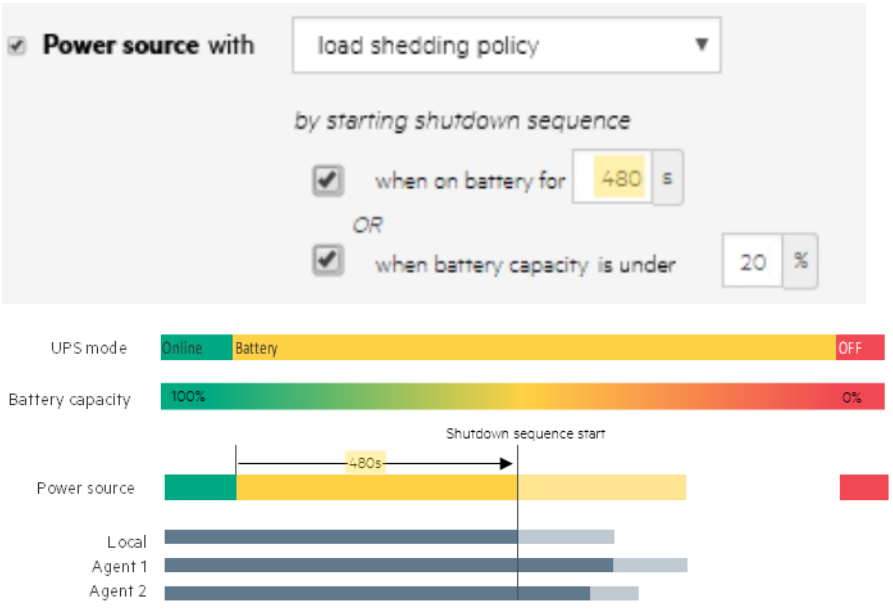


- Example 2: Immediate graceful shutdown policy

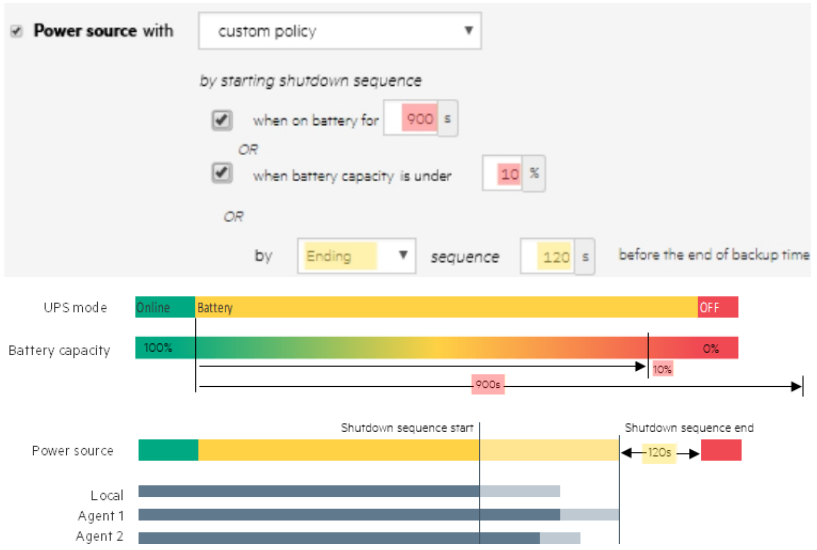




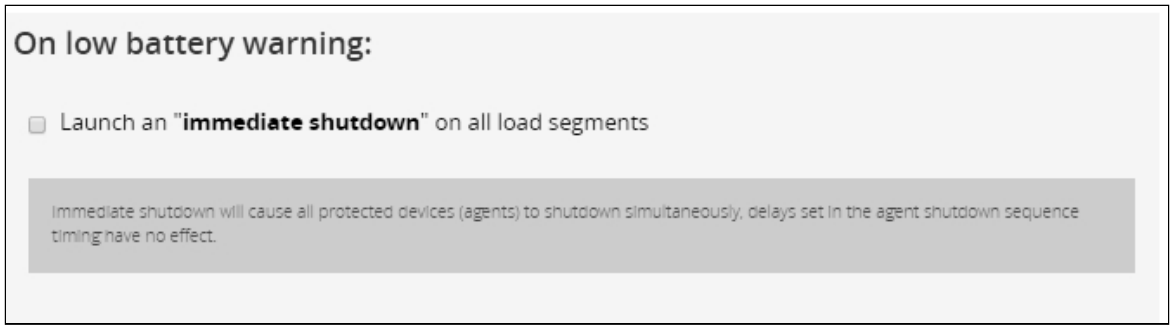
- Example 3: Load shedding policy

Settings #1	
Settings #2	

- Example 4: Custom policy

Settings #1	
Settings #2	

On low battery warning

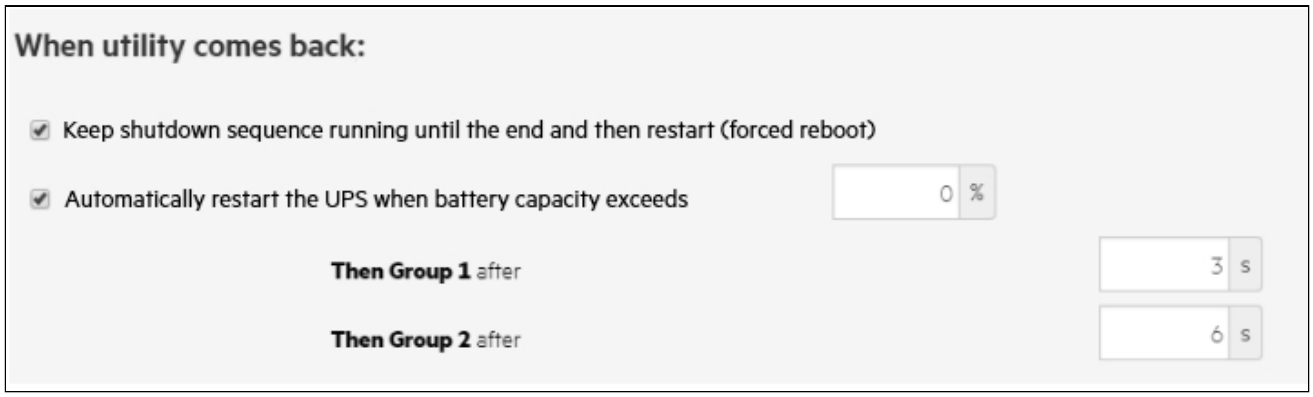


In some cases, like a renewed power failure or failed battery, the capacity is much lower than anticipated. The UPS gives a Low battery warning when there is 2 - 3 minutes of estimated runtime left, depending on the UPS and its

settings. This time is typically enough for shutting down a server but does not allow sophisticated sequential shutdown schemes.

The Low battery policy is intended for these cases.

When utility comes back



These settings define the restart sequence when utility comes back. For example, this allows sequential startup of the IT system so that network and storage devices are connected to 'Primary' and start up immediately. After a delay database servers in Group1 are powered up, and then application and web servers in Group 2 are powered up. This startup would ensure that necessary services would be available for each layer when needed. A sequential startup will also help avoid a peak power draw in the beginning.

Options

- Keep shutdown sequence running until the end, and then restart (forced reboot).
- Wait until UPS battery capacity exceeds a set percentage value in (%), and then automatically restart the UPS.

  - Then restart Group 1 after a set time in (s).

  - Then restart Group 2 after a set time in (s).

Enable/Disable

Each option listed above can be enabled or disabled with check-boxes.

When disabled, the option will be greyed out.

2.8 Card

2.8.1 System information

System information is an overview of the main Network Module information.

The **COPY TO CLIPBOARD** button will copy the information to the clipboard.

Identification

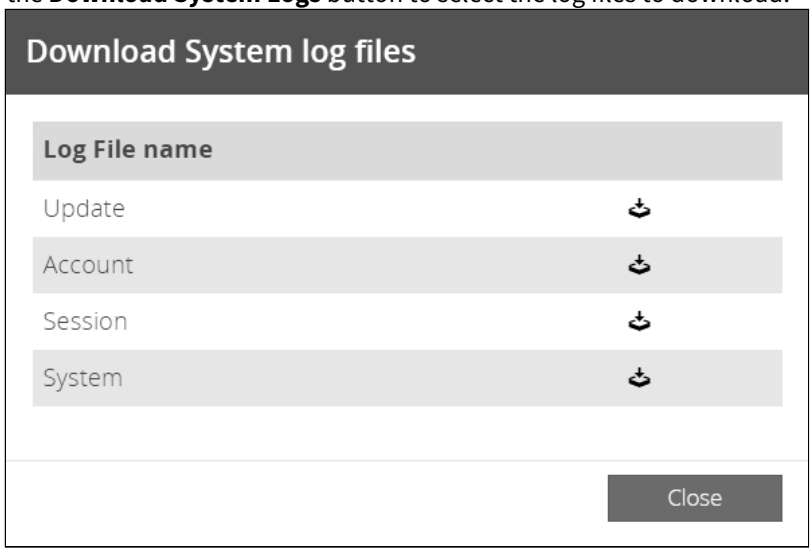
- System name – if filled, it replaces the UPS model name in the top bar
- Product
- Physical name
- Vendor
- UUID
- Part number
- Serial number
- Hardware version
- Location
- Contact

Firmware information

- Version
- SHA
- Build date
- Installation date
- Activation date
- Bootloader version

2.8.2 System logs

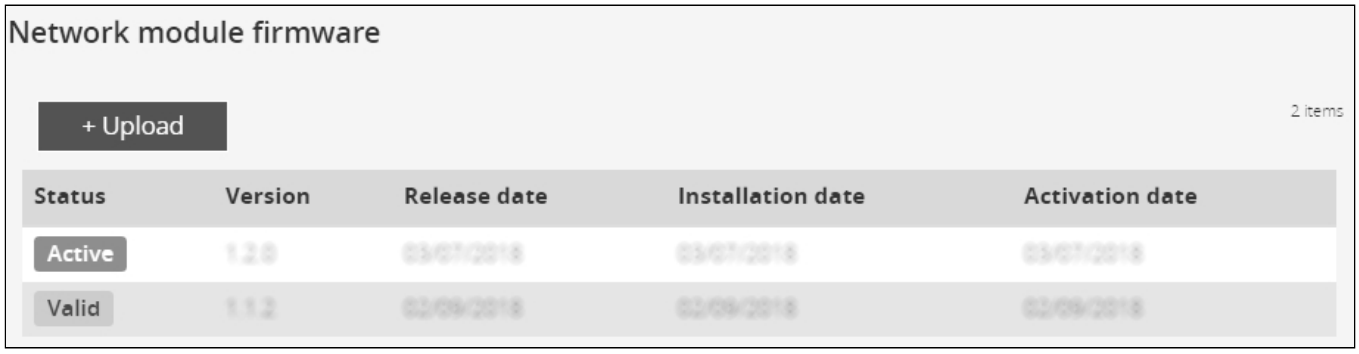
Press the **Download System Logs** button to select the log files to download.



For the list of system logs, see the **Information>>>System Logs codes** section.

2.8.3 Administration

Network module firmware



- Monitors the information for the two-embedded firmware.
- Upgrade the Network Module firmware.

Firmware information

Status
- Uploading
- Invalid
- Valid
- Pending reboot
- Active

Version
Displays the associated firmware version.

Release date
Displays the release date of the firmware.

For better performance, security, and optimized features,Eaton recommends to upgrade the Network Module regularly.

Installation date
Displays when the firmware was installed in the Network Module.

Activation date
Displays when the firmware was activated in the Network Module.

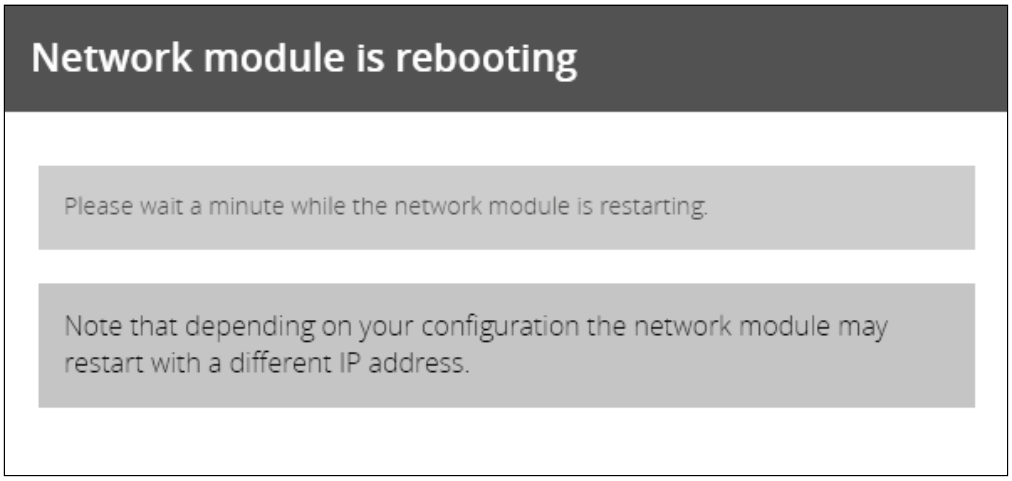
Upgrade the Network Module firmware

During the upgrade process, the Network Module does not monitor the UPS Product status.

To upgrade the firmware:

1. Download the latest firmware version from the website. For more information, see the ***Servicing the Network Management Module>>>Accessing to the latest Network Module firmware/driver*** section .
2. Click **+Upload**.
3. Select the firmware package by navigating to the folder where you saved the downloaded firmware.
4. Click **Upload**. The upload can take up to 5 minutes.

- The firmware that was inactive will be erased by this operation.
- When an upgrade is in progress, the upload button is disabled, and the progress elements appear below the table with the following steps:
  Transferring > Verifying package > Flashing > Configuring system > Rebooting
- A confirmation message displays when the firmware upload is successful, and the UPS Network Module automatically restarts.



> ***Do not close the web browser or interrupt the operation.***
> ***Depending on your network configuration, the Network Module may restart with a different IP address.***
> ***Refresh the browser after the Network module reboot time to get access to the login page.***
> ***Press F5 or CTRL+F5 to empty the browser to get all the new features displayed on the Web user interface.***
> ***Communication Lost and Communication recovered may appear in the Alarm section.***

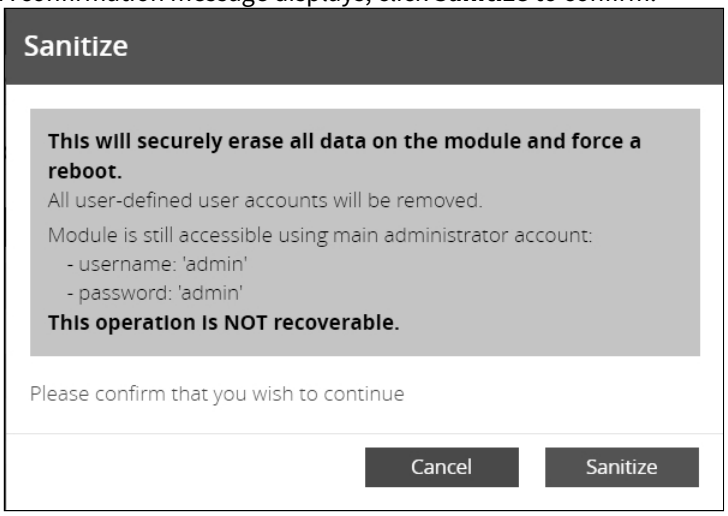
Sanitization

Sanitization removes all the data; the Network Module will come back to factory default settings.

> For details on default settings, see the ***Information>>>Default settings parameters*** section .

To sanitize the Network Module:

1. Click **Sanitize**.
2. A confirmation message displays, click **Sanitize** to confirm.



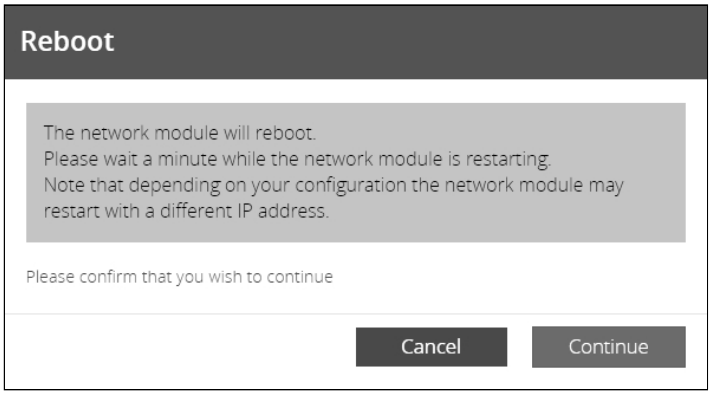
> ***Depending on your network configuration, the Network Module may restart with a different IP address.***
> ***Only main administrator user will remain with default login and password.***
> ***Refresh the browser after the Network module reboot time to get access to the login page.***

Reboot

Reboot means restarting the network module operating system.

To reboot the Network Module:

1. Click **Reboot**.
2. A confirmation message displays, click **Continue** to confirm, the reboot time will take approximately less than 2min.



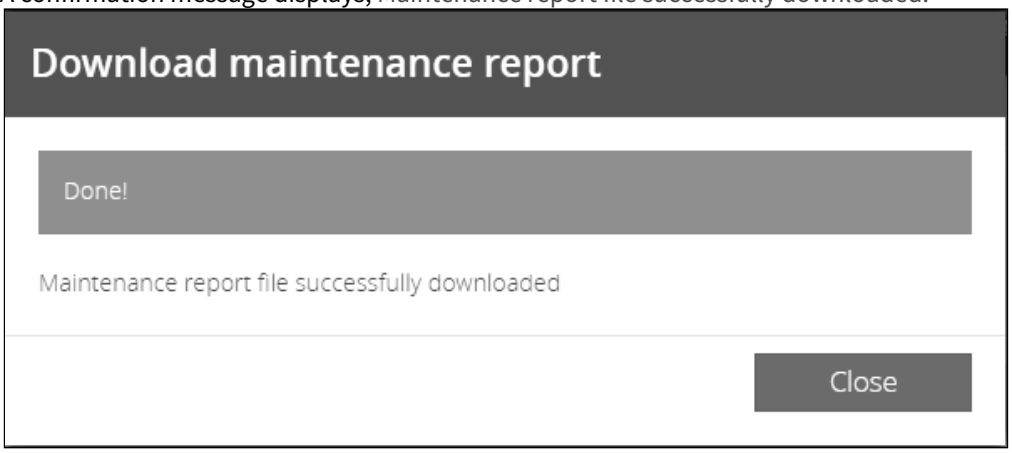
> ⚠ ***Depending on your network configuration, the Network Module may restart with a different IP address. Refresh the browser after the Network module reboot time to get access to the login page. Communication Lost and Communication recovered may appear in the Alarm section.***

Maintenance

The maintenance report is for the service representative use to diagnose problems with the network module. It is not intended for the user, which is why the file is protected by a password. None of the network module users or network information are extracted.

To download the maintenance report file:

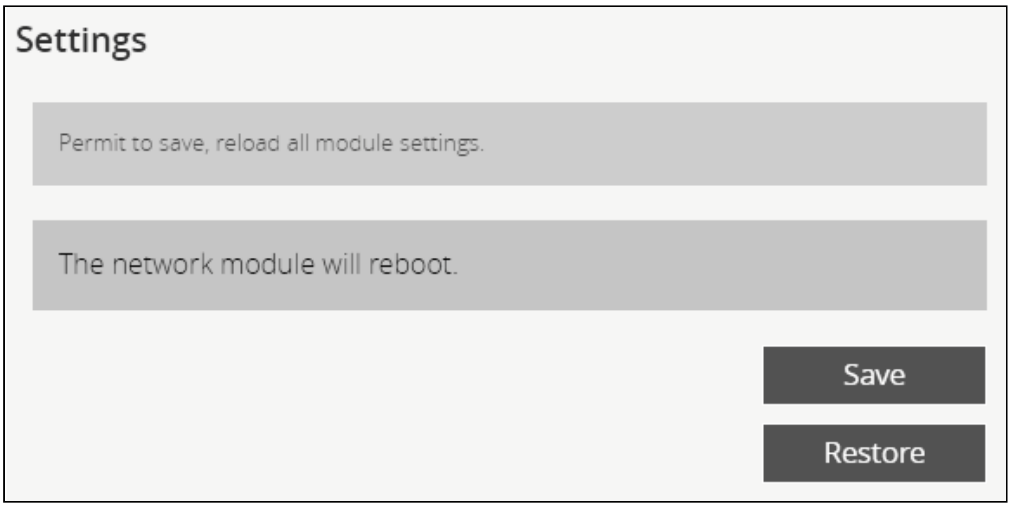
1. Click **Download report**.
2. A confirmation message displays, Maintenance report file successfully downloaded.



Settings

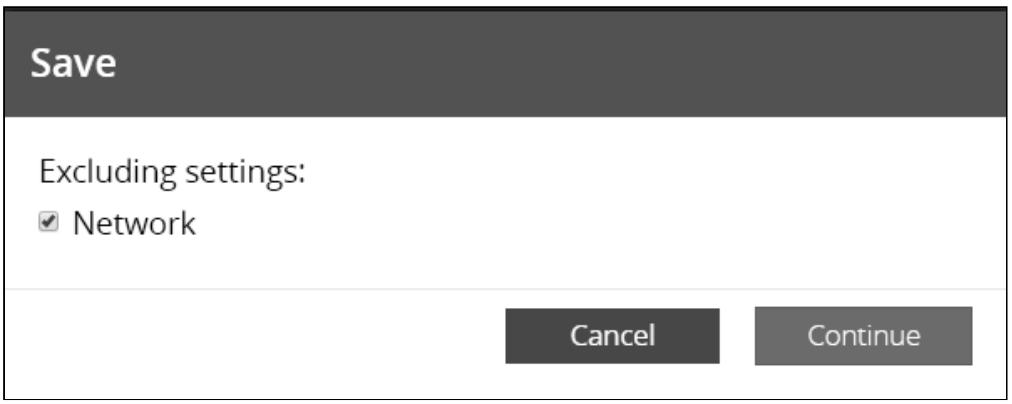
Allow to save and restore the Network module settings.

> ⓘ For more details, navigate to ***Servicing the Network Management Module>>>Saving/Restoring/Duplicating*** Network module configuration settings.



Save

> ⚠ Below settings are not saved:
> - Protection agents (agent list, agent settings)
> - Sensor settings (commissioning, alarm configuration)

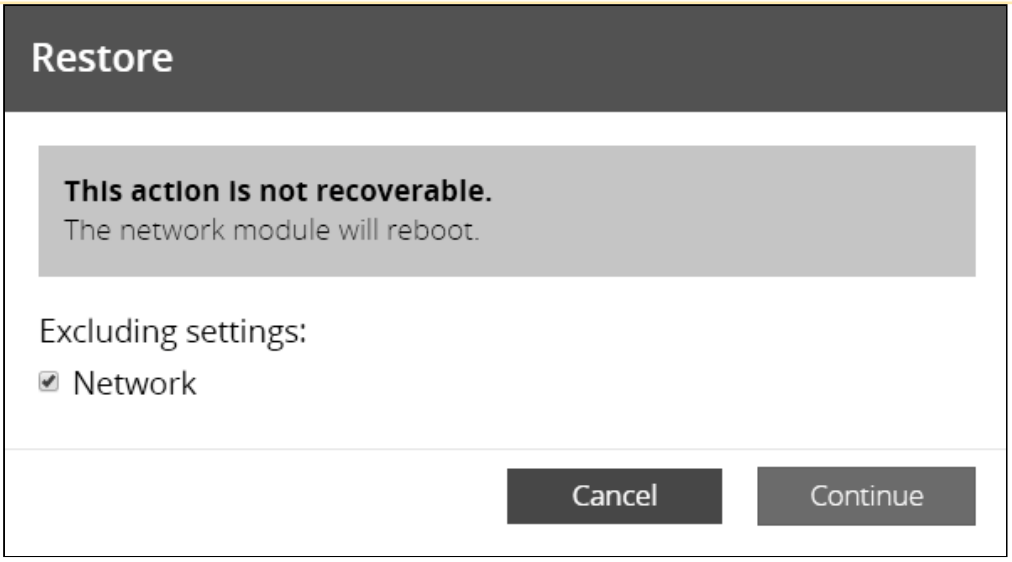


To save the Network module settings:

1. Click on **Save**
2. Select to include the Network settings if needed.
3. A passphrase need to be entered twice to cypher the sensitive data.
4. Click on **Continue**

Restore

⚠ Restoring settings may result in the Network module reboot.

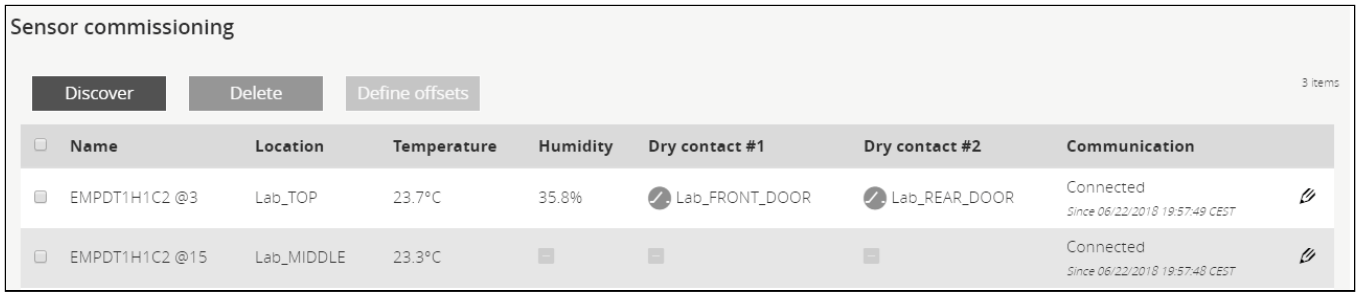


To restore the Network module settings:

1. Click on **Restore**
2. Select to include the Network settings if needed.
3. Click on **Continue**
4. Select the JSON file
5. If sensitive data are detected, enter the passphrase used when the file was saved.
6. Click again on **Continue** to confirm

2.8.4 Commissioning (sensors)

Sensors commissioning table



The table displays the sensors commissioning information and includes the following details.

- **Name**
- **Location –** location-position-elevation
- **Temperature**
- **Humidity**
- **Dry contact #1 –** Status and name
- **Dry contact #2 –** Status and name

Polarity set	Current state	Dry contact status
Normally open	open	
Normally open	closed	
Normally closed	closed	
Normally closed	open	

- **Communication –** Connected/Lost with dates

Actions

Discover

At first the table is empty, press the **Discover** button to launch the sensor discovery process.

If sensors are discovered, the table is populated accordingly

Delete

Select a sensor and press the **Delete** button to delete the sensor.

⚠ When a sensor is deleted, all the commissioning information are deleted.

Define offsets

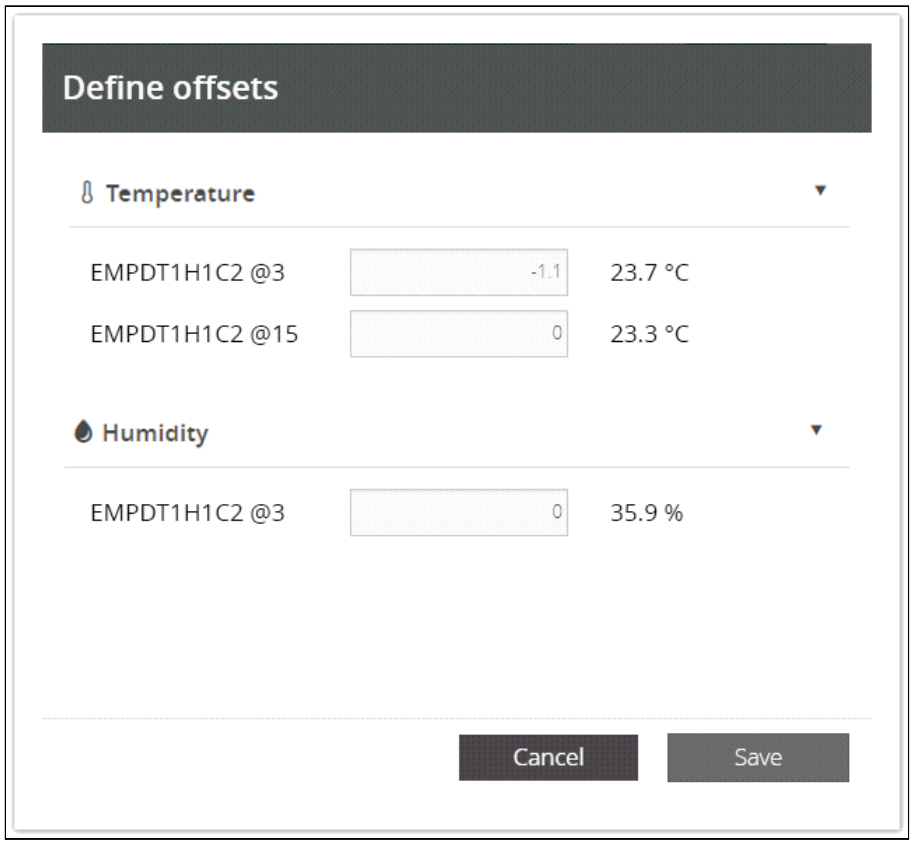
Select the sensors.

Press the **Define offset** button to adjust the temperature and humidity offsets of the selected sensors.

Extend the temperature or humidity section.

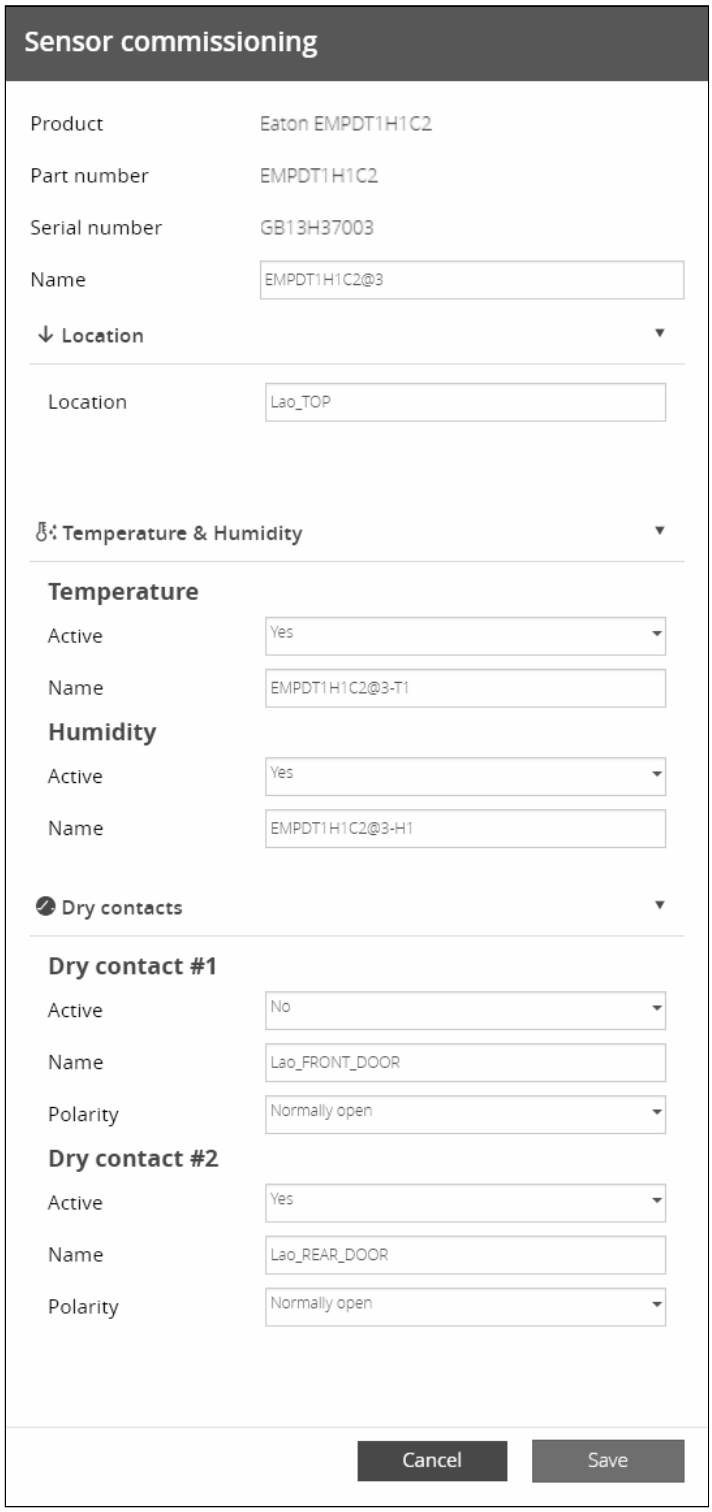
Set the offsets in the cell, temperatures and humidity will be updated accordingly.

Press the **Save** button when done.



Deactivated humidity or temperatures are not displayed.

Edit



Press the pen logo to edit sensor communication information and access to the following information and settings:

- Product reference
- Part number
- Serial number
- Name
- Location
- Temperature and humidity – Active (Yes, No)
- Dry contacts – Active (Yes, No)/Name/Polarity (Normally open, Normally closed)

Press **Save** after modifications.

Note:

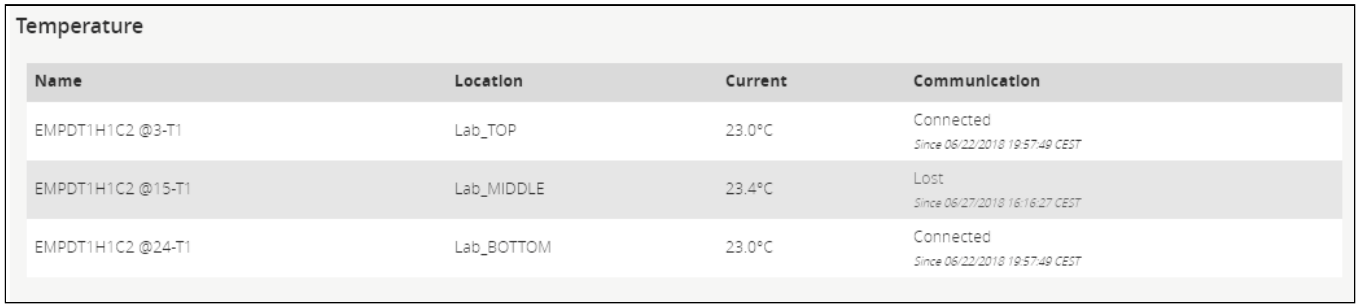
If the UPS provides temperature compensated battery charging option, see the ***Servicing the EMP>>>Using the EMP for temperature compensated battery charging*** section

2.9 Sensors

2.9.1 Status (sensors)

Humidities, temperatures or dry contacts deactivated during commissioning are not displayed.

Temperature table

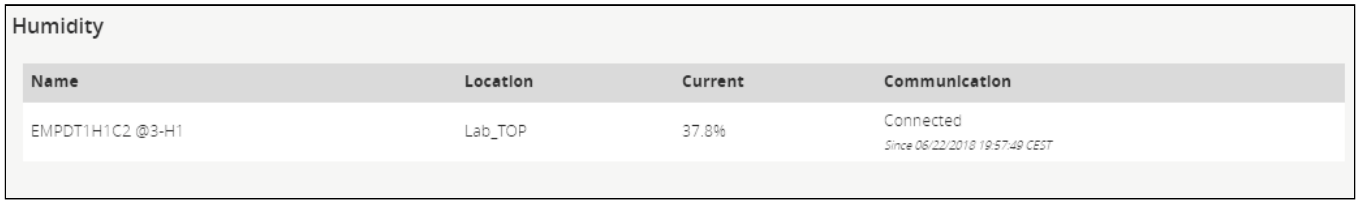

Temperature

Name	Location	Current	Communication
EMPDT1H1C2 @3-T1	Lab_TOP	23.0°C	Connected *Since 06/22/2018 19:57:49 CEST*
EMPDT1H1C2 @15-T1	Lab_MIDDLE	23.4°C	Lost *Since 06/27/2018 16:16:27 CEST*
EMPDT1H1C2 @24-T1	Lab_BOTTOM	23.0°C	Connected *Since 06/22/2018 19:57:49 CEST*

The table shows the following information for each sensor.

- Name
- Location
- Current temperature
- Communication – Connected/Lost with dates

Humidity table

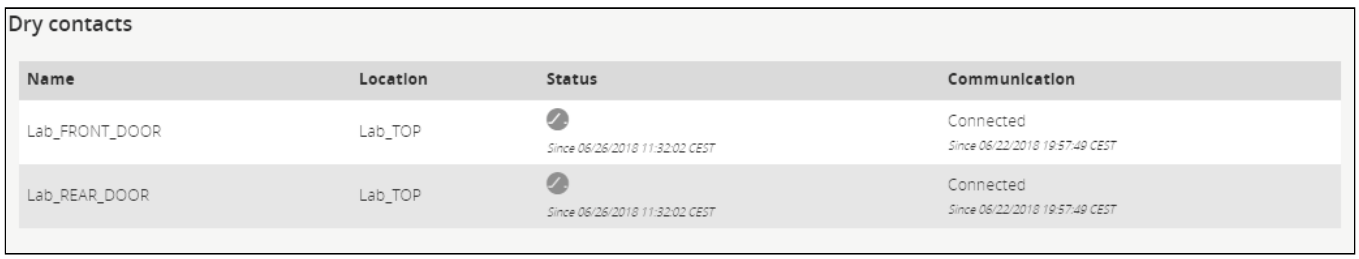

Humidity

Name	Location	Current	Communication
EMPDT1H1C2 @3-H1	Lab_TOP	37.8%	Connected *Since 06/22/2018 19:57:49 CEST*

The table shows the following information for each sensor.

- Name
- Location
- Current humidity
- Communication – Connected/Lost with dates

Dry contacts table


Dry contacts

Name	Location	Status	Communication
Lab_FRONT_DOOR	Lab_TOP	*Since 06/26/2018 11:32:02 CEST*	Connected *Since 06/22/2018 19:57:49 CEST*
Lab_REAR_DOOR	Lab_TOP	*Since 06/26/2018 11:32:02 CEST*	Connected *Since 06/22/2018 19:57:49 CEST*

The table shows the following information for dry contacts.

- Name
- Location
- Status with date

Polarity set	Current state	Dry contact status
Normally open	open	
Normally open	closed	
Normally closed	closed	
Normally closed	open	

- Communication – Connected/Lost with dates

2.9.2 Alarm configuration (sensors)

Humidity, temperatures or dry contacts deactivated during commissioning are not displayed.

Temperature

The table shows the following information and settings for each sensor.

- Name
- Enabled – yes/no
- Low critical threshold – xx°C or xx°F
- Low warning threshold – xx°C or xx°F
- Current temperature
- High warning threshold – xx°C or xx°F
- High critical threshold – xx°C or xx°F
- Hysteresis – x°C or x°F

Actions

Set Enabled
Select and directly change the setting in the table and then **Save**.

When disabled, no alarm will be sent.

Set alarm threshold
Select and directly change the setting in the table and then **Save**.

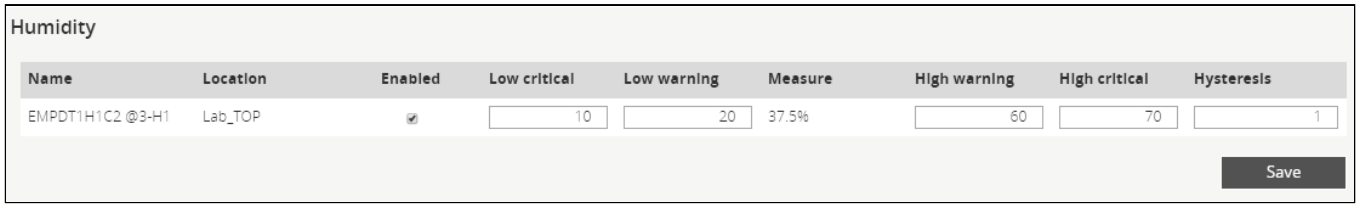
When a warning threshold is reached, an alarm will be sent with a warning level.

When a critical threshold is reached, an alarm will be sent with a critical level.

Set Hysteresis
Select and directly change the setting in the table and then **Save**.

The hysteresis is the difference between the value where the alarm turns ON from turning OFF and the value where it turns OFF from turning ON.

Humidity



The table shows the following information and settings for each sensor.

- Name
- Enabled – yes/no
- Low critical threshold – xx%
- Low warning threshold – xx%
- Current humidity
- High warning threshold – xx%
- High critical threshold – xx%
- Hysteresis – x%

Actions

Set Enabled
Select and directly change the setting in the table and then **Save**.

When disabled, no alarm will be sent.

Set alarm threshold
Select and directly change the setting in the table and then **Save**.

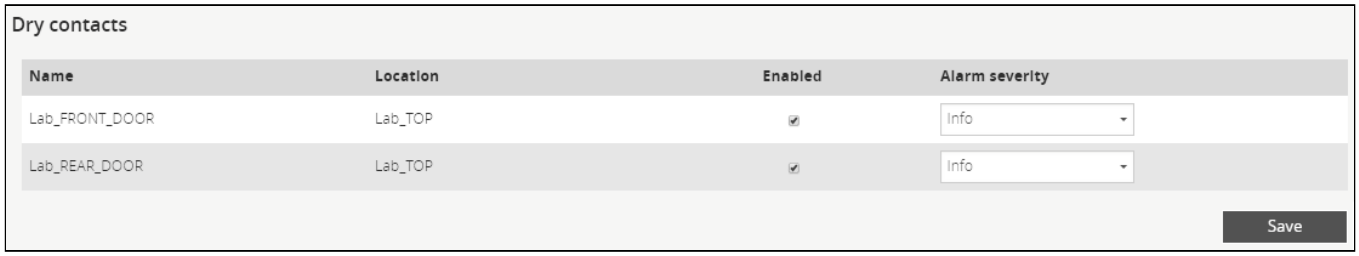
When a warning threshold is reached, an alarm will be sent with a warning level.

When a critical threshold is reached, an alarm will be sent with a critical level.

Set Hysteresis
Select and directly change the setting in the table and then **Save**.

The hysteresis is the difference between the value where the alarm turns ON from turning OFF and the value where it turns OFF from turning ON.

Dry contacts



The table shows the following settings for each dry contact.

- Name
- Enabled – yes/no
- Alarm severity – Info/Warning/Critical

Actions

Set Enabled
Select and directly change the setting in the table and then **Save**.

When disabled, no alarm will be sent.

Set alarm severity
Select and directly change the setting in the table and then **Save**.

Dry contacts alarm will be sent at the selected level.

Default settings parameters and limitations

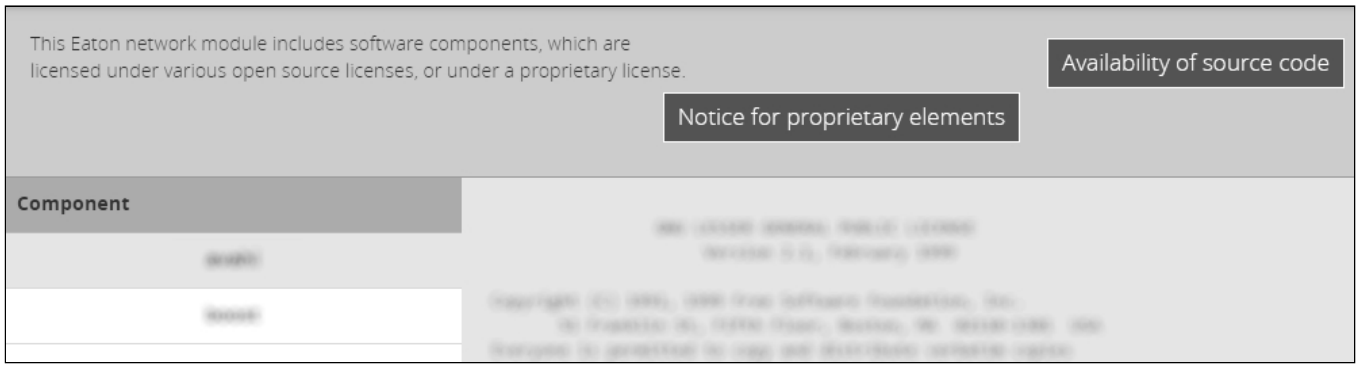
For details on default parameters and limitations, see the ***Information>>>Default settings parameters*** section

2.9.3 Information (sensors)

Sensor information is an overview of all the sensors information connected to the Network Module.

- Physical name
- Vendor
- Part number
- Firmware version
- UUID
- Serial number
- Location

2.10 Legal information (footer)



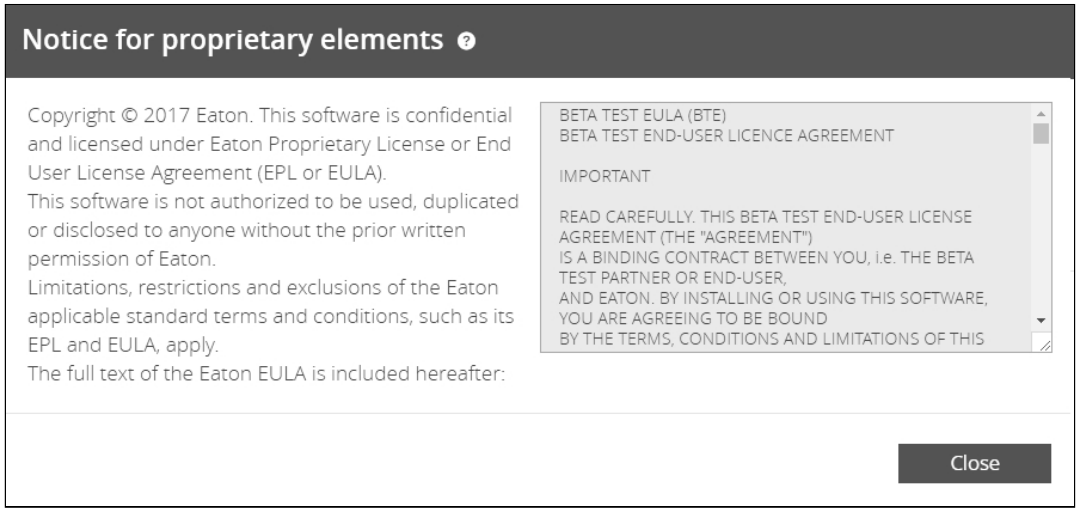
This Network Module includes software components that are either licensed under various open source license, or under a proprietary license.

2.10.1 Component list

All the open source components included in the Network Module are listed with their licenses.

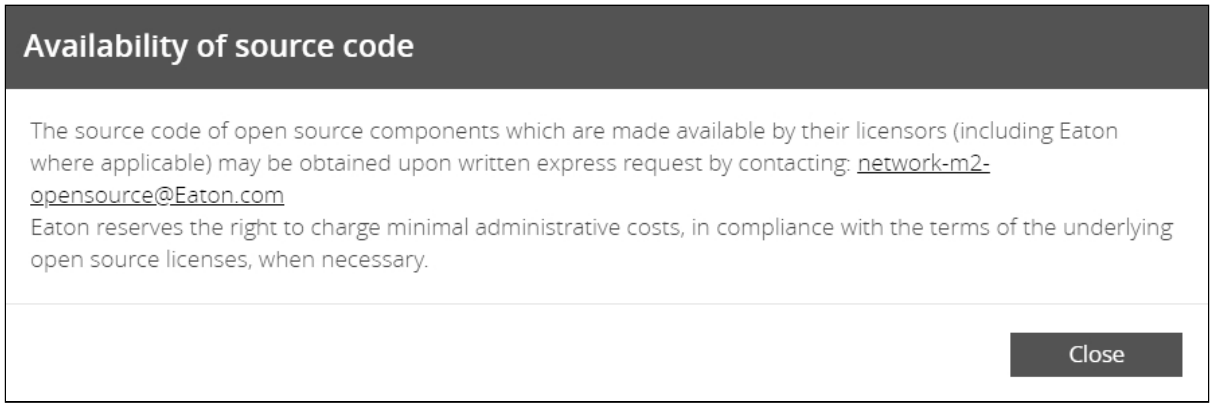
2.10.2 Notice for our proprietary (i.e. non-Open source) elements

Provides notice for our proprietary (i.e. non-Open source) elements.



2.10.3 Availability of source code

Provides the way to obtain the source code of open source components that are made available by their licensors.



2.11 Contextual help and full documentation

2.11.1 Access to contextual help

Press **?** icon on the top right side of the page to access the contextual help.

Contextual help can be closed by pressing the **X** icon on the top right of the page.

Search feature is indexed, but when inside the contextual help section it won't search in the full documentation.
To get better results when searching, search inside the full documentation.

2.11.2 Access to full documentation

Press **?** icon on the top right side of the page to access the contextual help.

In the contextual help section, press the **Full documentation** button on the top right to access the full documentation in a new window.

You can then navigate into below sections:

- Contextual help
- Servicing the Network Management Module
- Securing the Network Management Module
- Information
- Troubleshooting

3 Servicing the Network Management Module

3.1 Unpacking the Network module

The network module will include the following:

- Network module
- QuickStart
- USB AM to Micro USB/M/5P 5ft Cable

> Packing materials must be disposed of in compliance with all local regulations concerning waste.
> Recycling symbols are printed on the packing materials to facilitate sorting.

3.2 Installing the Network Module

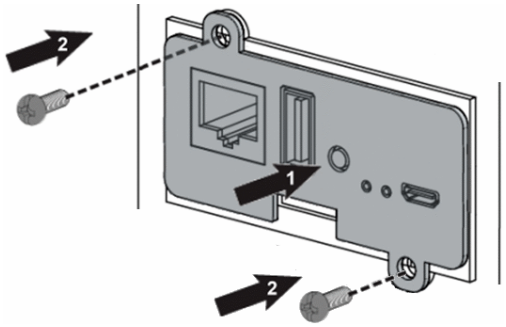
3.2.1 Mounting the Network Module

> It is not necessary to power down the UPS before installing the Network Module. Required tools: No. 2 Phillips screwdriver.

The Network Module is hot-swappable. Inserting and/or extracting the Network Module from the communication slot of the product has no effect on the output.

Remove the two screws securing the option slot cover plate and store the plate for possible future use.

- Install the Network Module along the alignment channels in the option slot.
- Secure the Network Module using the two screws.



- If the product is powered up, you can verify that the Network Module is seated properly and communicating with the product by checking that the Status ON LED flashes green after 2 minutes.

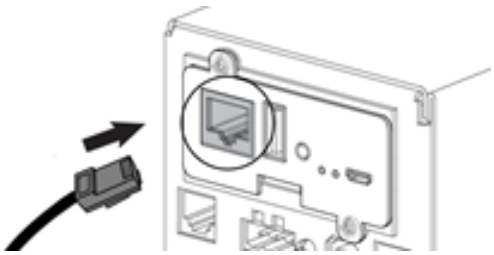
3.3 Accessing the Network Module

3.3.1 Accessing the web interface through Network

Connecting the network cable

> Security settings in the Network Module may be in their default states.
> For maximum security, configure through a USB connection before connecting the network cable.

Connect a standard *gigabit compatible shielded ethernet cable (F/UTP or F/FTP)* between the network connector on the Network Module and a network jack.



Accessing the web interface

It is highly recommended that browser access to the Network Module is isolated from outside access using a firewall or isolated network.

1. On a network computer, launch a supported web browser. The browser window appears.
2. In the Address/Location field, enter: https://xxx.xxx.xxx.xxx, where xxx.xxx.xxx.xxx is the static IP address of the Network Module.
   The log in screen appears.
3. Enter the user name in the User Name field. The default user name is **admin**.
4. Enter the password in the Password field. The default password is **admin**.
   The password must be changed at first login.
5. Click **Sign In**. The Network Module web interface appears.

3.3.2 Finding and setting the IP address

Your network is equipped with a BOOTP/DHCP server (default)

Read from the device LCD

Note: some older UPS may not be able to display the IP address even if they have an LCD. Please consult the UPS manual.

If your device has an LCD, from the LCD's menu, navigate to Identification>>>"COM card IPv4".

- Note the IP address of the card.
- Go to the section: Accessing the web interface through Network.

With web browser through the configuration port

For example, if your device does not have an LCD, the IP address can be discovered by accessing the web interface through RNDIS and browsing to Settings>Network.

- To access the web interface through RNDIS, see the Accessing the web interface through RNDIS section.
  - Navigate to Settings>>>Network>>>IPV4.
  - Read the IPv4 settings.

Your network is not equipped with a BOOTP/DHCP server

Define from the configuration port

The IP address can be defined by accessing the web interface through RNDIS.

To access web interface through RNDIS, see the Accessing the web interface through RNDIS section.

Define the IP settings:

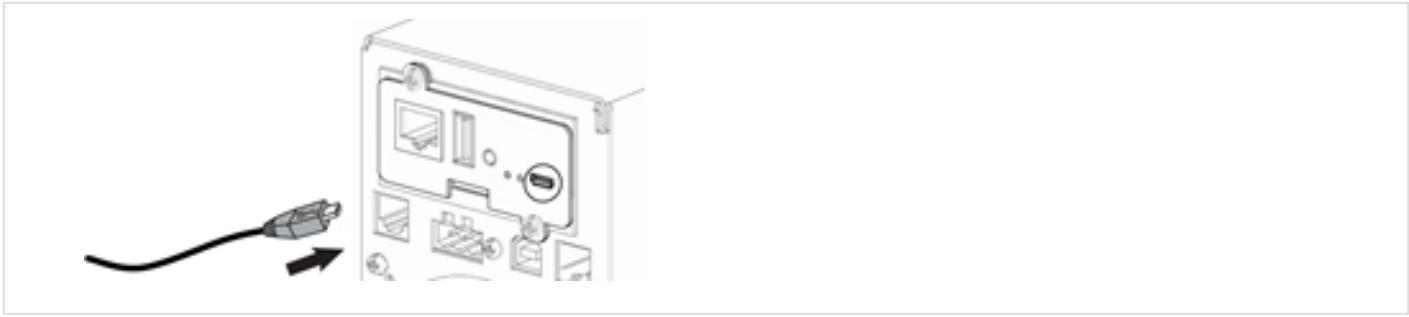
- Navigate to Settings>>>Network>>>IPV4.
- Select Manual (Static IP).
- Input the following information: Address, Subnet Mask, Default Gateway
- Save the changes.

3.3.3 Accessing the web interface through RNDIS

Connecting the configuration cable

1. Connect the Micro-B to USB cable to a USB connector on the host computer.

2. Connect the cable to the Settings connector on the Network Module.



This connection is used to access and configure the Network Module network settings locally through a RNDIS (Ethernet over USB interface).

Web interface access through RNDIS

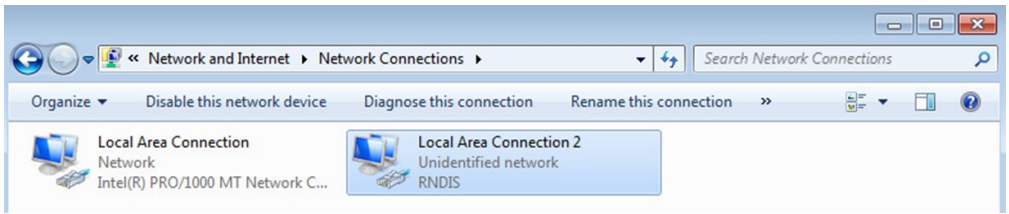
Configuring the RNDIS

Automatic configuration

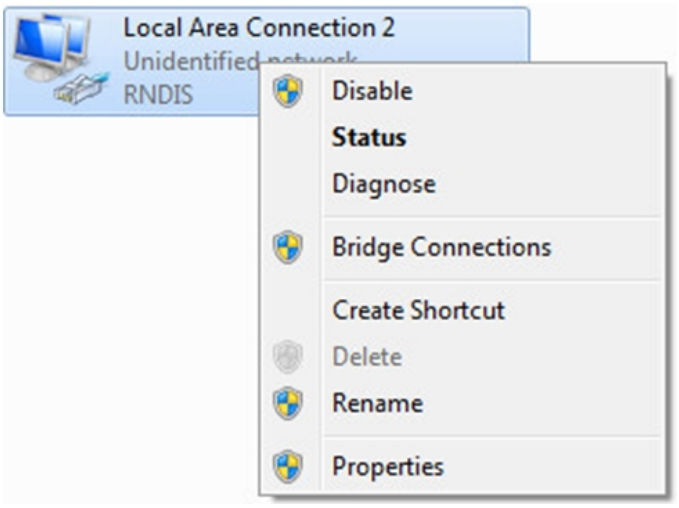
> RNDIS driver is used to emulate a network connection from USB.
> After the card is connected to the PC, **Windows**® OS will automatically search for the RNDIS driver.
> On some computers, the OS can find the RNDIS driver then configuration is completed, and you can go to Accessing the web interface.
> On some others it may fail then proceed to manual configuration.

Manual configuration

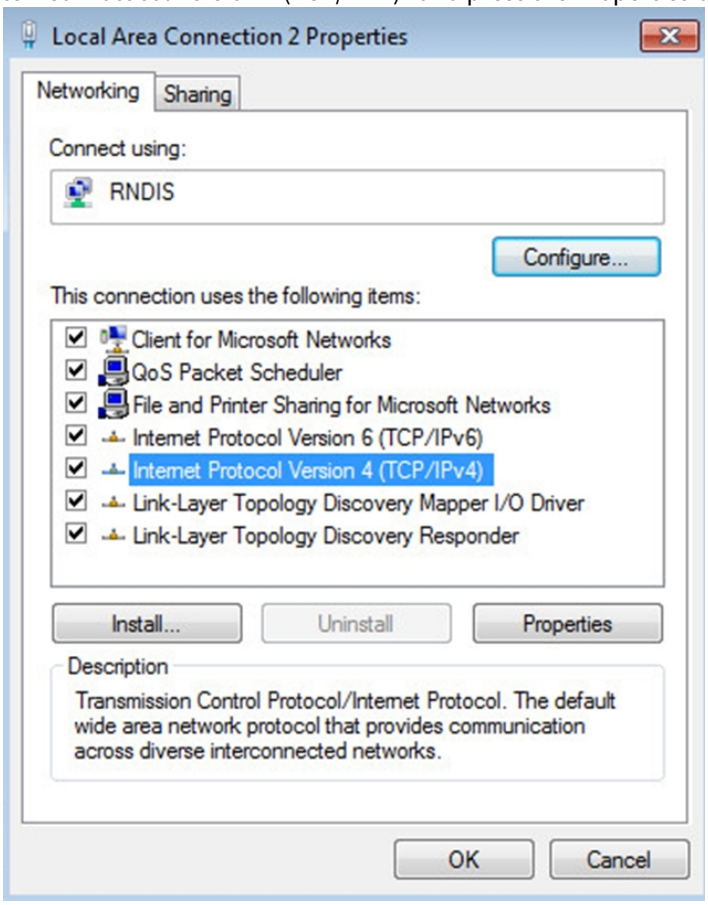
1. In case **Windows**® OS fails to find driver automatically, go to the Windows control panel>Network and sharing center>Local area connection



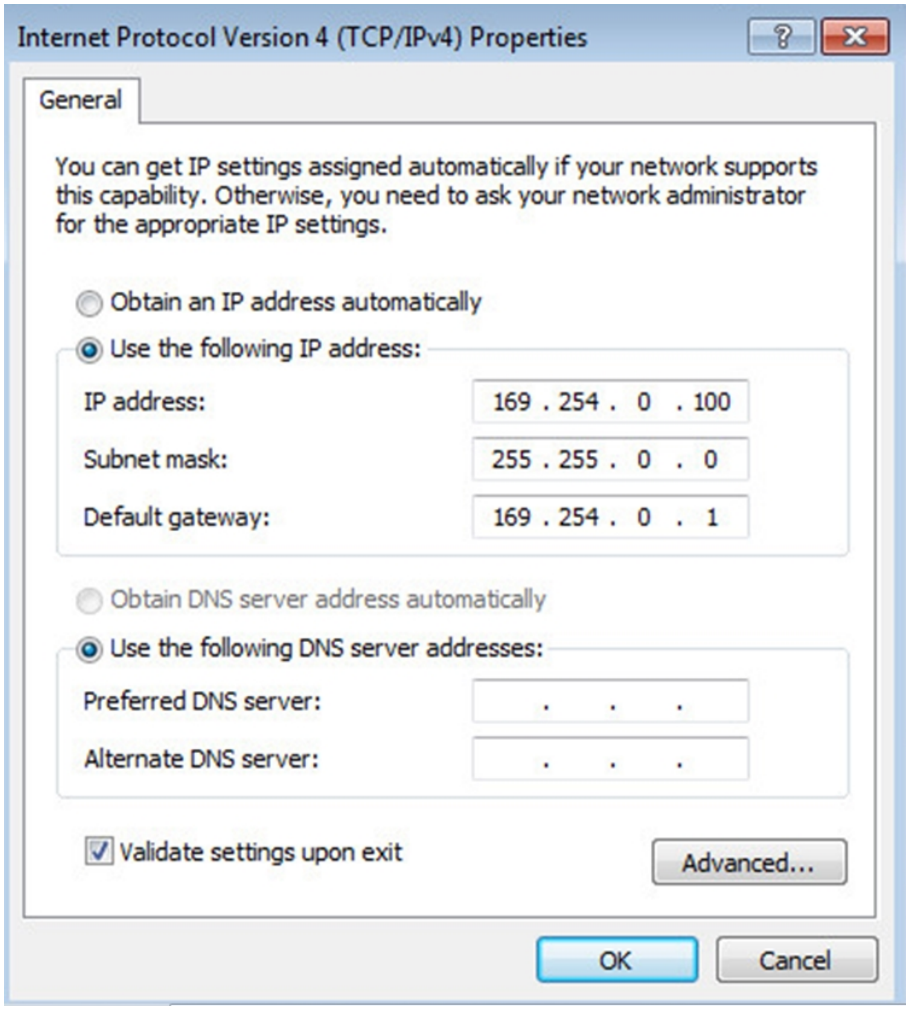
2. Right click on the RNDIS local area connection and select Properties.



3. Select Internet Protocol Version 4 (TCP/IPv4)" and press the Properties button.



4. Then enter the configuration as below and validate (IP = 169.254.0.150 and mask = 255.255.255.0), click OK, then click on Close.



Accessing the web interface

1. Be sure that the UPS is powered on.

2. On the host computer, download the rndis.7z file from the website www.powerquality.eaton.com/Support/ and extract it. For more information, navigate to Accessing to the latest Network Module firmware/driver section.

3. Launch setProxy.bat to add 169.254.* in proxy's exceptions list, if needed. For manual configuration, navigate to Modifying the Proxy exception list section in the full documentation.

4. Launch a supported browser, the browser window appears.

5. In the Address/Location field, enter: **https://169.254.0.1**, the static IP address of the Network Module for RNDIS. The log in screen appears.

6. Enter the user name in the User Name field. The default user name is **admin**.

7. Enter the password in the Password field. The default password is **admin**.

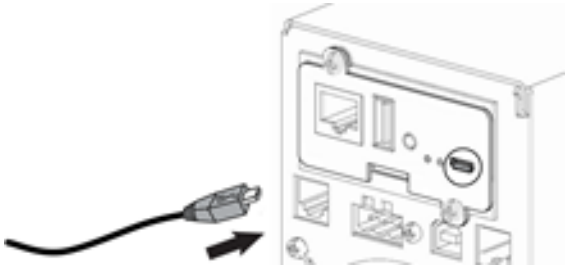
8. Click **Sign In**. The Network Module local web interface appears.

3.3.4 Accessing the card through serial terminal emulation

Connecting the configuration cable

1. Connect the Micro-B to USB cable to a USB connector on the host computer.

2. Connect the cable to the Settings connector on the Network Module.



This connection is used to access and configure the Network Module network settings locally through Serial (Serial over USB interface).

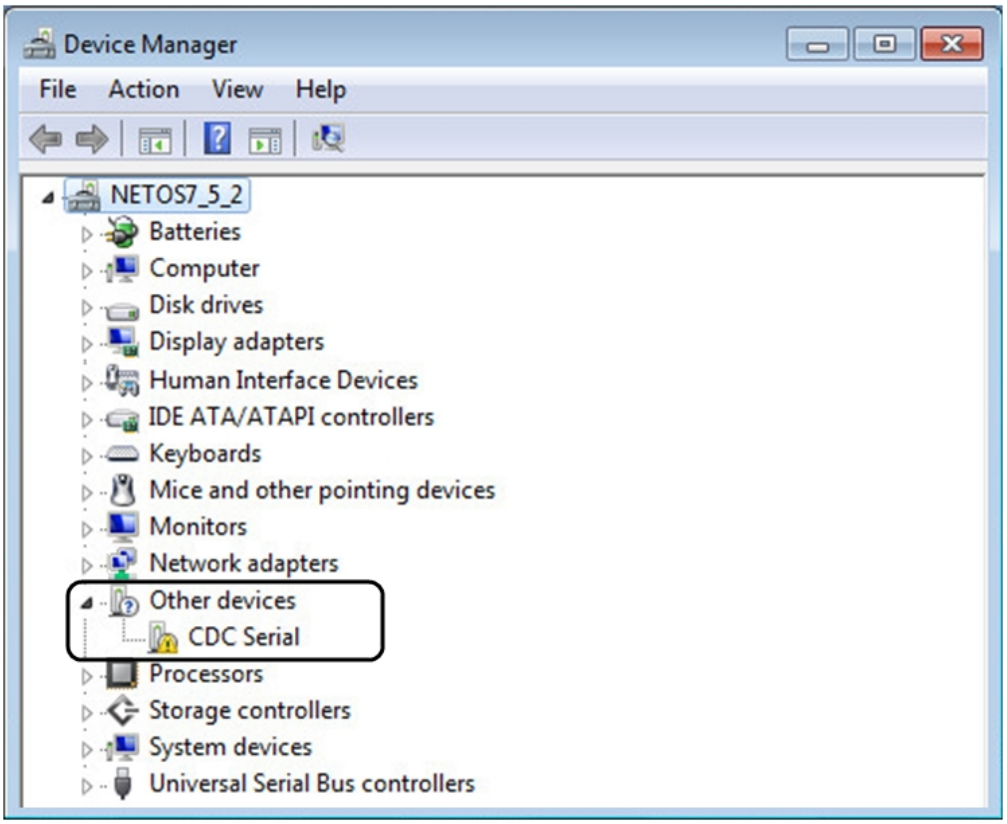
Manual configuration of the serial connection

Serial driver is used to emulate a serial connection from USB.
After the card is connected to the PC, manual configuration of the driver is needed for **Windows**® OS to discover the serial connection.

1. On the host computer, download the rndis.7z file from the website www.powerquality.eaton.com/Support/ and extract it.

2. Plug the USB cable and go to **Windows**® Device Manager.

3. Check the CDC Serial in the list, if it is with a yellow exclamation mark implying that driver has not been installed follow the steps 4-5-6-7 otherwise configuration is OK.

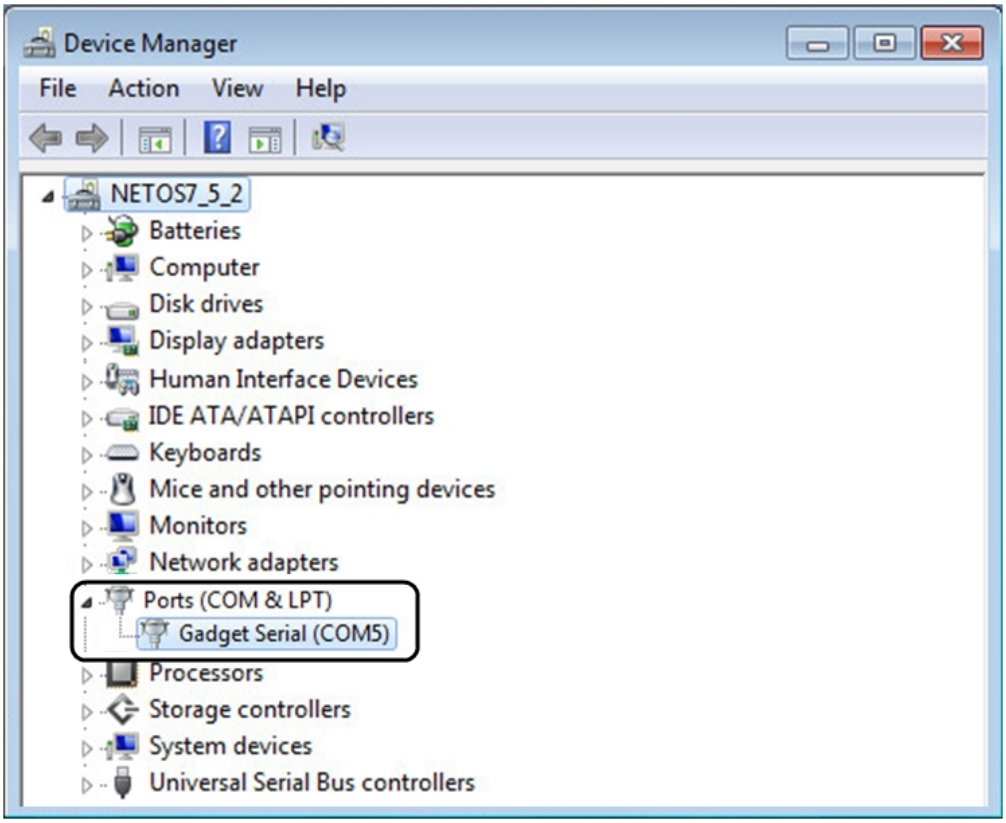


4. Right click on it and select Update Driver Software. When prompted to choose how to search for device driver software, choose Browse my computer for driver software. Select Let me pick from a list of device drivers on my computer.

5. Select the folder where you have previously downloaded the driver file Click on Next.

6. A warning window will come up because the driver is not signed. Select Install this driver software anyway

7. The installation is successful when the COM port number is displayed for the Gadget Serial device in the **Windows**® Device Manager.



Accessing the card through Serial

CLI can be accessed through:

- SSH
- Serial terminal emulation.

It is intended mainly for automated configuration of the network and time settings of the network card. It can also be used for troubleshooting and remote reboot/reset of the network interface in case the web user interface is not accessible.

⚠ Changing network parameters may cause the card to become unavailable remotely. If this happens it can only be reconfigured locally through USB.

ⓘ You can see this list of available commands by typing in the CLI: ***?***
You can see the help by typing in the CLI: ***help***

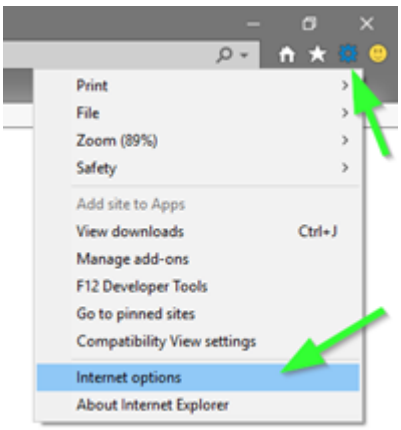
3.3.5 Modifying the Proxy exception list

To connect to the Network Module via a USB cable and your system uses a Proxy server to connect to the internet, the proxy settings can reject the IP address 169.254.0.1.

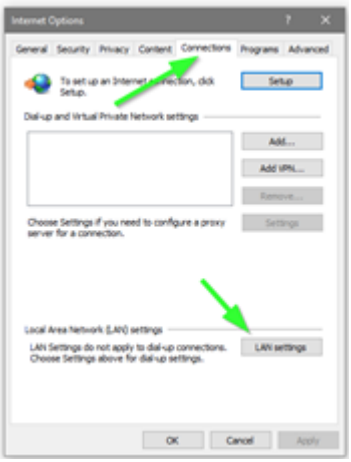
The 169.254. * Sequence is used to set up communication with devices via a physical connection.

To activate this connection, exceptions will have to be made in the proxy settings.

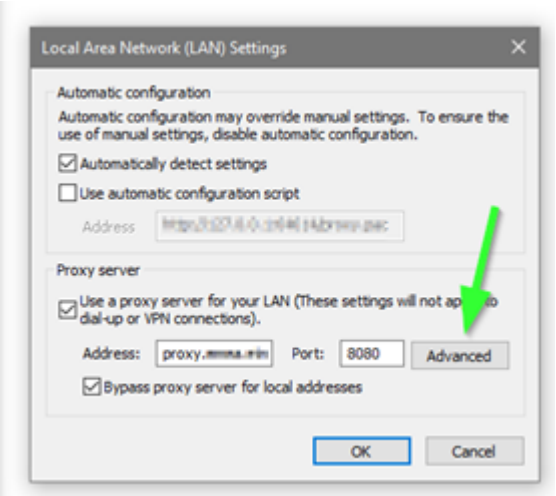
- Open Internet Explorer
- Navigate to settings, Internet options;



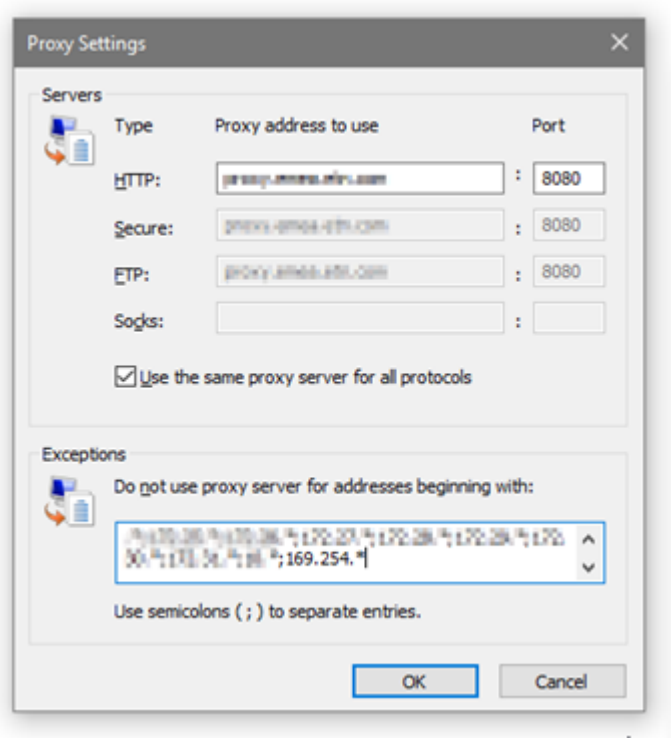
- Select the Connections tab
- Press LAN Settings



- Press ADVANCED



- Add the address 169.254. *



- Press OK.
- Close Internet Explorer and re-open it.
- Now you can access the address 169.254.0.1 with Internet Explorer and any other browser.

3.4 Configuring the Network Module settings

Use Eaton UPSNetwork Module web interface to configure the UPS Network Module.

Main web interface menus are described below:

	Home page with overview of the UPS/Module status (Synoptic with measures, Active alarms, Meters, Outlet status,…).
	Module settings (Date&Time, Users, Network, Protocols, Certificates, Email, My Preferences, …).
	List of Alarms with date, time and description.
	Power quality meters and measure logs.
	Entire UPS Control, Battery test, Outlets control.
	Scheduled Shutdown, Agents list, Agent Settings, Power Outage Policy.

	Sensors (only displayed when sensors have been discovered in card administration)
	Card administration (Firmware upgrade, reboot, save and restore, commissioning,...)

3.5 Configuring/Commissioning/Testing LDAP

3.5.1 Commissioning

Refer to the section Contextual Help>>>Settings>>>Users to get help on the configuration.

Configuring connection to LDAP database

This step configures the LDAP client of the network module to request data from an LDAP base.

1. Activate LDAP.
2. Define security parameters according to LDAP servers' requirements.
3. Configure primary server (and optionally a secondary one).
4. If security configuration needs server certificate verification, import your LDAP server certificate.
   Refer to the section to get help on certificate import.
   a. In case LDAP server certificate is self-signed, import the self-signed certificate in the *Trusted remote certificate* list **for *LDAP* service**.
   b. in case LDAP server certificate has been signed by a CA, import the corresponding CA in the *Certificate authorities (CA)* list **for *LDAP* service**.
5. Configure credentials to bind with the LDAP server or select *anonymous* if no credentials are required.
6. Configure the *Search base DN*.
7. Configure the request parameters (see examples below).

Typical request parameters

Parameter	**OpenLDAP**	**Active Directory™ with POSIX account activated**	**Active Directory™**
User base DN	ou=users, dc=example, dc=com	ou=users, dc=example, dc=com	ou=users, dc=example, dc=com
User name attribute	uid	uid	sAMAccountName
UID attribute	uidNumber	uidNumber	objectSid:S-1-5-xx-yy-zz (domain SID)
Group base DN	ou=groups, dc=example, dc=com	ou=groups, dc=example, dc=com	ou=groups, dc=example, dc=com
Group name attribute	gid	gid	sAMAccountName
GID attribute	gidNumber	gidNumber	objectSid:S-1-5-xx-yy-zz (domain SID)

Testing connection to LDAP database

Refer to the section Information>>>CLI>>>ldap-test to get help on the CLI command.

To test connection to the LDAP database:

1. Connect to the CLI.
2. Launch *ldap-test --checkusername* command.
3. In case of error, use the *verbose* option of the command to investigate the reason.

Map remote users to profile

> This step is mandatory and configures the Network module to give permissions to the LDAP users.
> Users not belonging to a group mapped on a profile will be rejected.

Configure the rules to mapped LDAP users to profile:

1. Enter LDAP group name.
2. Select the profile to assigned.

You can define up to 5 mapping rules.

All LDAP users belonging to the configured LDAP group will have permissions granted by the associated profile.

> If a user belongs to multiple LDAP groups mapped to different profiles, the behavior is undefined.

Testing profile mapping

Refer to the section Information>>>CLI>>>ldap-test to get help on the CLI command.

To test LDAP users profile mapping:

1. Connect to the CLI.
2. Launch *ldap-test --checkmappedgroups* command.
3. This command will verify each mapped group exists in the LDAP base and will display the associated local profile.
4. In case of error, use the *verbose* option of the command to investigate the reason.

Define LDAP user's preferences

This step configures the user's preferences to apply to **all** LDAP users.

3.5.2 Testing LDAP authentication

Refer to the section Information>>>CLI>>>ldap-test to get help on the CLI command.

1. Connect to the CLI.
2. Launch *ldap-test --checkauth* command.
3. This command will verify an LDAP user can authenticate using his username and password and will display its local profile.
4. In case of error, use the *verbose* option of the command to investigate the reason

3.5.3 Limitations

- If the same username exists in both local and LDAP databases, the behavior is undefined.
- If a user belongs to multiple LDAP groups mapped to different profiles, the behavior is undefined.
- No client certificate provided. It is not possible for the server to verify the client authenticity.
- It is not possible to configure LDAP to work with 2 different search bases.
- LDAP user's preferences are common to **all** LDAP users.
- LDAP users cannot change their password through the Network Module.

3.6 Pairing agent to the Network Module

Authentication and encryption of connections between the UPS network module and shutdown agents is based on matching certificates.

3.6.1 Pairing with credentials on the agent

STEP 1: Action on the agent (IPP or IPM).

1. Connect to the web interface of the agent.

2. Detect the UPS Network Module with an **Address(es) scan**, select Override global authentication settings and type the UPS Network Module credentials.

3.6.2 Pairing with automatic acceptance (recommended if done in a secure and trusted network)

Pairing with automatic acceptance of shutdown agents and UPS network modules is recommended in case the installation is done in a secure and trusted network, and when certificates cannot be created in other ways.

STEP 1: Action on the Network Module

1. Connect to the Network Module

   - On a network computer, launch a supported web browser. The browser window appears.
   - In the Address/Location field, enter: https://xxx.xxx.xxx.xxx where xxx.xxx.xxx.xxx is the static IP address of the Network Module.
   - The log in screen appears.
   - Enter the user name in the User Name field.
   - Enter the password in the Password field.
   - Click **Sign In**. The Network Module web interface appears.

2. Navigate to **Protection/Agents list** page

3. In the **Pairing with shutdown agents** section, select the time to accept new agents and press the **Start** button and the press **Continue**. During the selected timeframe, new agent connections to the Network Module are automatically trusted and accepted.

STEP 2: Action on the agent (IPP) while the time to accepts new agents is running on the Network Module

1. Connect to the web interface of the agent.

2. Detect the UPS Network Module with a **Quick scan**, **Range scan** or an **Address(es) scan**.

3. Right-click on the UPS Network Module when discovered and then **Set as power source**, **Configure** it, and **Save** it.

STEP 3: Action on the Network Module

1. Make sure all listed agents in the card (**Protection/Agents list**) belong to your infrastructure, if not, access may be revoked using the **Delete** button.

2. If the time for pairing still runs, you can stop it. Press **Stop** in the **Pairing with shutdown agents** section.

ⓘ **STEP 1** and **STEP2** can be done either ways.

3.6.3 Pairing with manual acceptance

Manual pairing provides the maximum security.

STEP 1: Action on the agent (IPP)

1. Connect to the web interface of the agent

2. Detect the UPS Network Module with a **Quick scan**, **Range scan** or an **Address(es) scan**.

3. Define the power source

Note: After that stage, the agent creates a client certificate. The power source could show a communication loss since the current client certificate is not trusted by the Network Module.

4. Copy the agent certificate file **client.pem** that is located in the folder Eaton\IntelligentPowerProtector\configs\tls.

STEP 2: Action on the Network Module

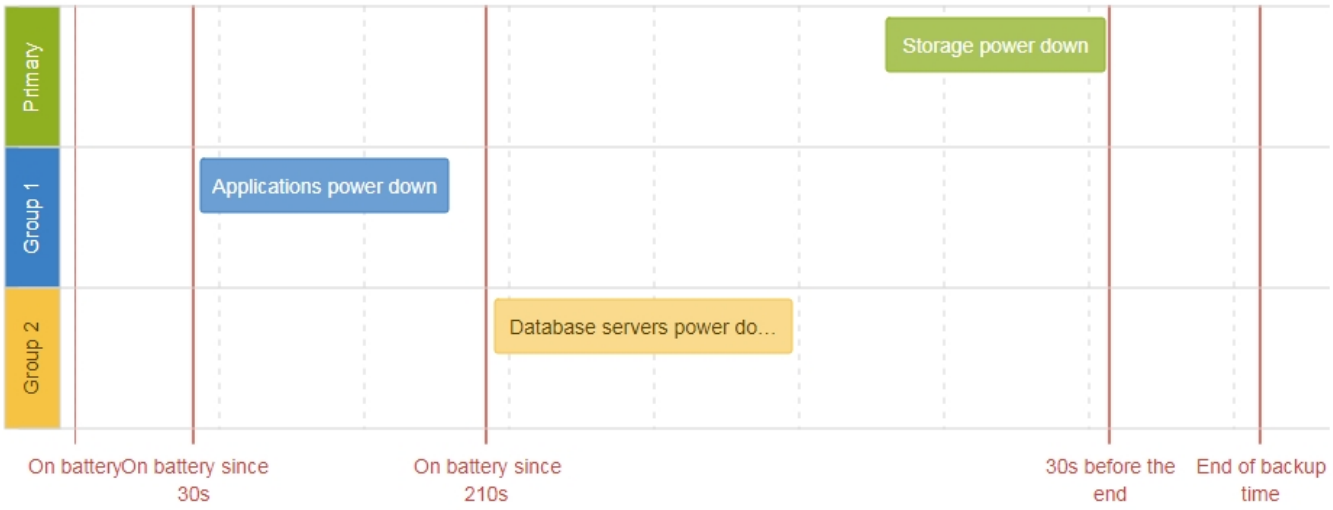
1. Connect to the Network Module
   - On a network computer, launch a supported web browser. The browser window appears.
   - In the Address/Location field, enter: https://xxx.xxx.xxx.xxx where xxx.xxx.xxx.xxx is the static IP address of the Network Module.
   - The log in screen appears.
   - Enter the user name in the User Name field.
   - Enter the password in the Password field.
   - Click **Sign In**. The Network Module web interface appears.
2. Navigate to **Settings/Certificate** page
3. In the **Trusted remote certificates section**, click **Import,** select **Protected applications (MQTT)** and then click on **CONTINUE**
4. Select the **client.pem** file previously saved, click **Open**. Communication with the agent is restored.

3.7 Powering down/up applications (examples)

3.7.1 Powering down IT system in a specific order

Target

Powering down applications first (when on battery for 30s), database servers next (3min after the applications), and storage last (as late as possible).



Step 1: Installation setup

Objective

Use load segmentation provided by the UPS to independently control the power supply of each IT equipment categories (Applications, Database servers, Storage).

It also allows IT equipment to sequentially restart on utility recovery (Restart sequentially the IT equipment on utility recovery).

Resulting setup

UPS provides outlets (Group 1 and Group 2) and a primary output.

⚠ When primary shuts OFF, both group 1 and group 2 shut OFF immediately.

Connections to UPS are done as described below:

- Group 1: Applications
- Group 2: Database servers
- Primary: Storage

Step 2: Agent settings

Objective

Ensure IT solution is shutdown gracefully.

Resulting setup

1. Install IPP Software on each server (Application, Database servers, Storage) and register the UPS load segment as power source:

   - Applications: Group 1
   - Database servers: Group 2
   - Storage: Entire UPS

2. Pair agent to the Network Module (Pairing agent to the Network Module).

   When done, each server appears in the Agent list.

3. Navigate to **Protection/Agent settings** page.

ⓘ For examples of Agent settings, see the Agent settings examples section.

4. Set the OS shutdown duration to the time needed for your server to shutdown gracefully.

   This will make sure IPP shutdowns your servers before the load segment is powered down.

   As a result, it will define the overall shutdown sequence duration for each load segments.

Step 3: Power outage policy settings

Objective

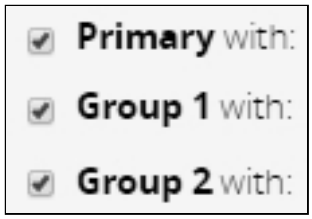
Use load segment policies to define shutdown sequencing.

Resulting setup

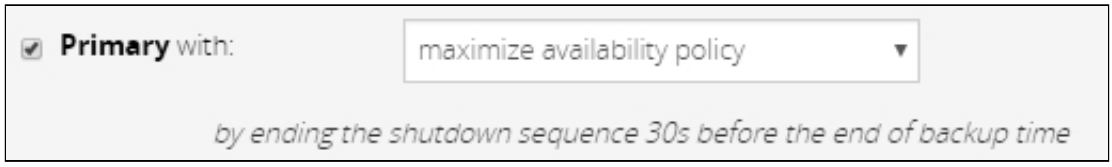
1. Navigate to **Protection/Power outage policy** page of the Network Module

ⓘ For examples of Power outage policy, see the following sections:
- Maximize availability policy example
- Immediate graceful shutdown policy example
- Load shedding policy examples
- Custom policy examples

2. Enable policies of Primary, Group 1 and Group 2.



3. Set Primary to: **maximize availability policy**.

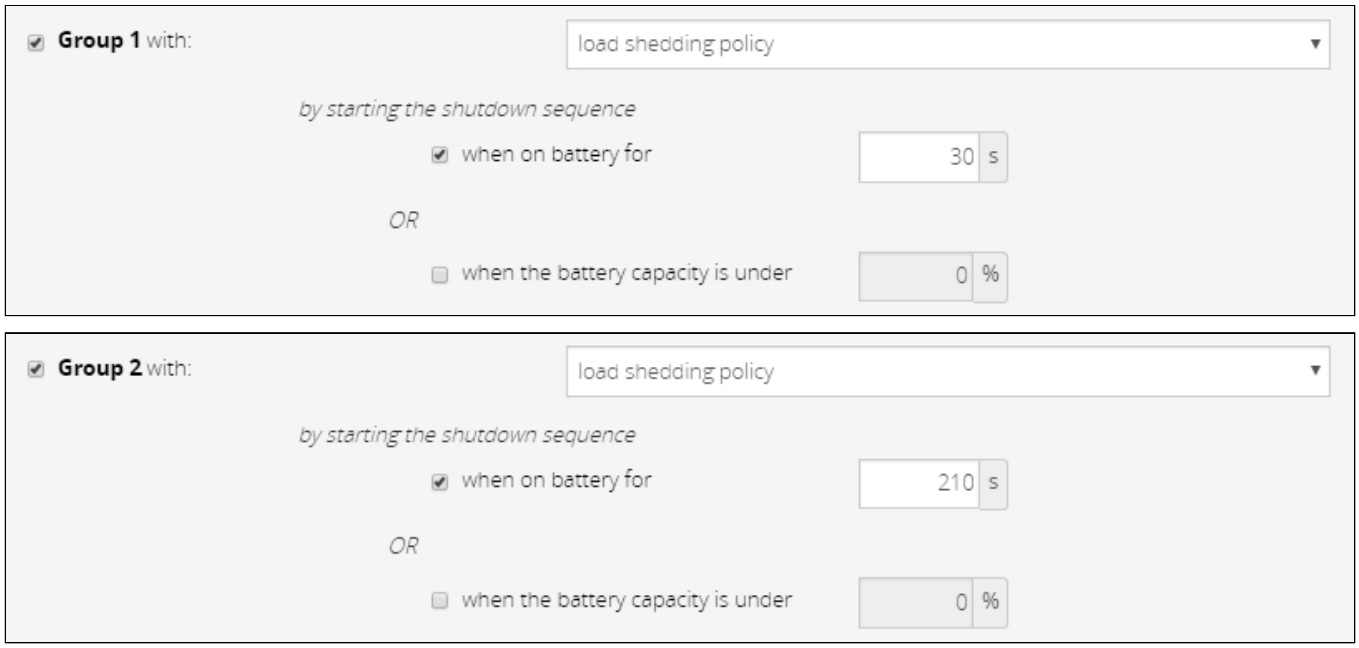


Storage is the last one to power down, its availability is maximized, and its shutdown will end 30s before the end of backup time.

4. Set Group 1 and Group 2 to: **load shedding policy**.

Applications must shutdown first so Group 1 has been set to start shutdown when on battery for 30s.

Servers must shutdown second, so Group 2 has been set to start shutdown when on battery for 210s, so 3min after the applications.

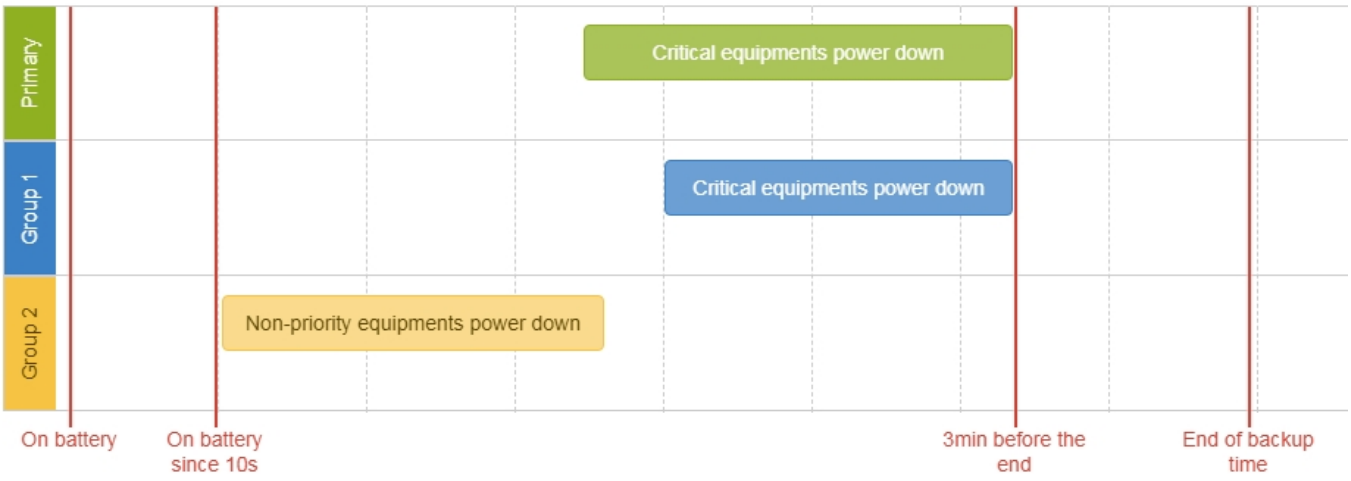


3.7.2 Powering down non-priority equipment first

Target

Powering down non-priority equipment first (immediately) and keep battery power for critical equipment.

Powering down critical equipment 3min before the end of backup time.



Step 1: Installation setup

Objective

Use load segmentation provided by the UPS to independently control the power supply of each IT equipment categories (Applications, Database servers, Storage).

Load segmentation also allows IT equipment to restart sequentially on utility recovery (Restart sequentially the IT equipment on utility recovery).

Resulting setup

UPS provides outlets (Group 1 and Group 2) and a primary output.

⚠ When primary shuts OFF, both group 1 and group 2 shut OFF immediately.

Connections can be done as described below:

- Group 2: non-priority equipment
- Group 1: critical equipment
- Primary: critical equipment

Step 2: Agent settings

Objective

Ensure IT solution is shutdown gracefully.

Resulting setup

1. Install IPP Software on each server (Application, Database servers, Storage) and register the UPS load segment as power source:

- Critical equipment: Group 1
- Non-priority equipment: Group 2
- Critical equipment: Entire UPS

2. Pair agent to the Network Module (Pairing agent to the Network Module).

When done, each server appears in the Agent list.

3. Navigate to **Protection/Agent settings** page

ⓘ For examples of Agent settings, see the Agent settings examples sections.

4. Set the OS shutdown duration to the time needed for your server to shutdown gracefully.

This will make sure IPP shutdowns your servers before the load segment is powered down.

As a result, it will define the overall shutdown sequence duration for each load segments.

Step 3: Power outage policy settings

Objective

Use load segment policies to define shutdown sequencing.

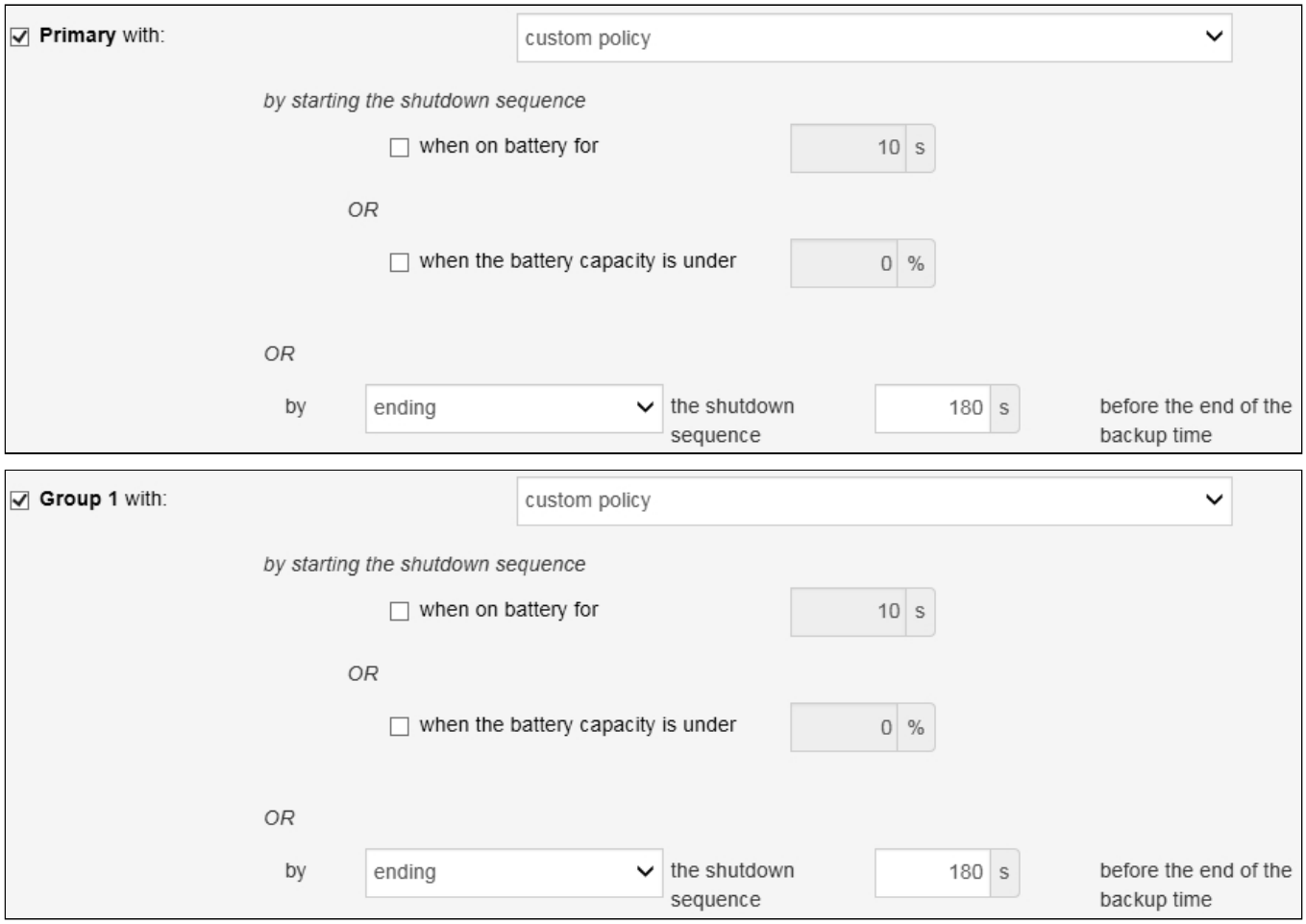
Resulting setup

1. Navigate to **Protection/Power outage policy** page on the Network Module

> For examples of Power outage policy, see the following sections:
> - Maximize availability policy example
> - Immediate graceful shutdown policy example
> - Load shedding policy examples
> - Custom policy examples

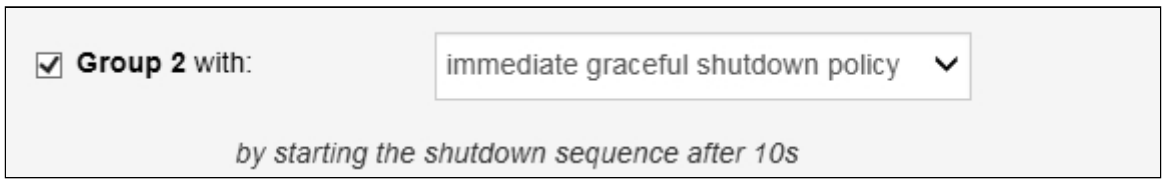
2. Enable policies of Primary, Group 1 and Group 2.

3. Set Primary and Group 1 to: **custom policy** and set it to end shutdown sequence 180s before the end of backup time.



Critical equipment is the last one to power down, their availability will be maximized and their shutdown will end 180s before the end of backup time.

4. Set Group 2 to: **immediate graceful shutdown policy**.

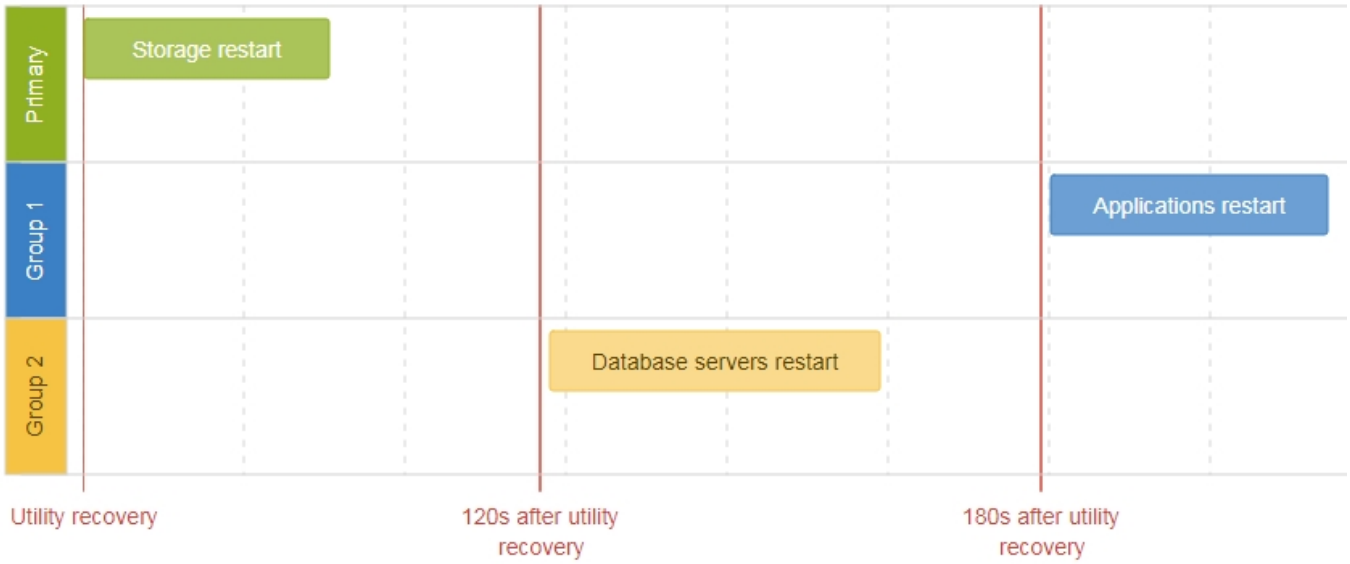


Non-priority equipment immediately shuts down when on battery for 10s to keep battery power for critical equipment.

3.7.3 Restart sequentially the IT equipment on utility recovery

Target

Restart the storage first (right after utility recovery), database servers next (2min after utility recovery) and applications last (3min after utility recovery).



Step 1: Installation setup

Objective

Use load segmentation provided by the UPS to independently control the power supply of each IT equipment categories (Applications, Database servers, Storage).

This will allow to restart sequentially the IT equipment on utility recovery.

Resulting setup

UPS provides outlets (Group 1 and Group 2) and a primary output.

⚠ When utility recovers, primary starts immediately.

Connections to UPS can be done as described below:

- Group 1: Applications
- Group 2: Database servers
- Primary: Storage

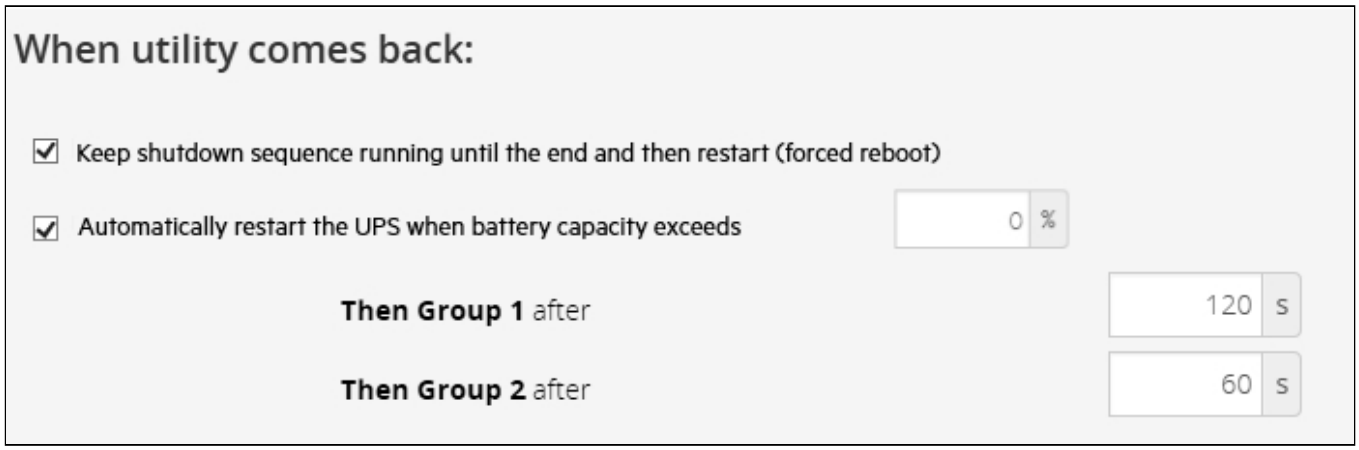
Step 2: Power outage policy settings

Objective

Use load segment restart settings to define restart sequencing.

Resulting setup

1. Navigate to **Protection/Power outage policy** page and to the **When utility comes back** section.



2. Enable the "Keep shutdown sequence running until the end and then restart (forced reboot)".
3. Enable the "Automatically restart the UPS when battery capacity exceeds" and set it to 0%.

   The storage will restart first, right after utility recovery without waiting the battery capacity to exceed a % limit.
4. Set Then Group 1 after to 120s.

   The database servers will restart 120s after the utility recovery.
5. Set Then Group 2 after to 60s.

   The database servers will restart 180s after the utility recovery.

3.8 Checking the current firmware version of the Network Module

Current firmware of the Network Module can be accessed in :

- The footer: Version : x.xx.x
- The Card menu : Card>>>System information>>>FW information: Firmware version x.xx.x
- The Card menu : Card>>>Administration>>>Network module firmware: Active FW version x.xx.x

3.9 Accessing to the latest Network Module firmware/driver/script

Download the latest Eaton Network Module firmware, driver or script from the Eaton website www.powerquality.eaton.com/Support/.

3.10 Upgrading the card firmware (Web interface / shell script)

For instructions on accessing to the latest firmware and script, refer to: Accessing to the latest firmware and script

3.10.1 Web interface

To upgrade the Network module through the Web interface, refer to the section: Firmware upgrade through the Web interface.

3.10.2 Shell script

Prerequisite

Shell script uses the following tools: sshpass, scp.

To get it installed on your Linux host, use the following commands.

Debian/Ubuntu

```
$ sudo apt-get install sshpass scp
```

RedHat/Fedora/CentOS

```
$ sudo dnf install sshpass scp
```

Make shell script executable:

```
$ chmod 700 install_updatePackage.sh
```

Procedure

To upgrade the Network module using:

1. Open a shell terminal on your computer (Linux or cygwin; meaning real or emulated Linux operating system).
2. Use the shell script *install_updatePackage.sh*

```
Usage: 'install_updatePackage.sh' [options]
Upgrade tool
Mandatory arguments are -f, -i, -u and -p
-h : show help
-f <path> : path of the upgrade file
-u <username> : username of a card user allowed to start upgrade
-p <password> : user password
-i <ipaddress> : ip address of the card to upgrade
-r : reboot the card after upgrade
```

3.10.3 Example:

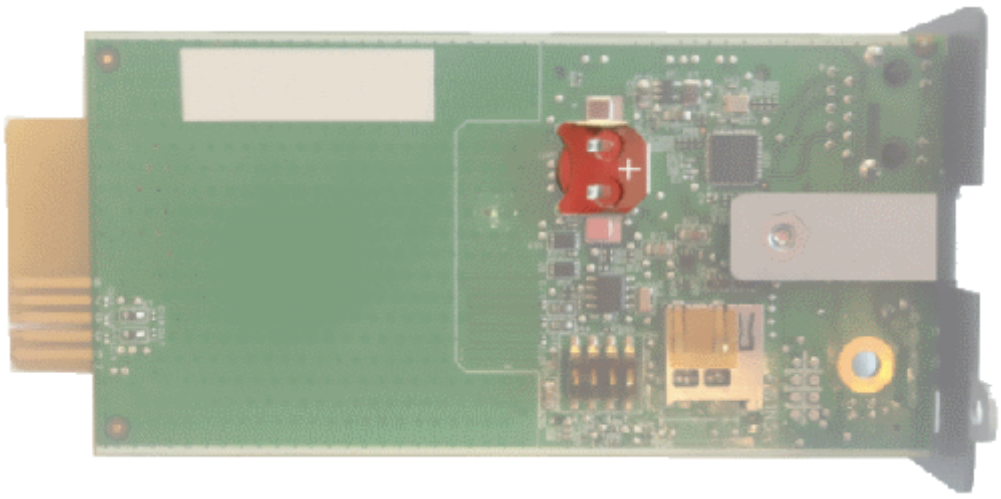
```
$ ./install_updatePackage.sh -u admin -p <mypassword> -f FW_Update.tar -i <cardIpAddress> -r
```

```
STARTING UPDATE FROM: [FW_Update.tar] to [X.X.X.X]

Transfer by scp (FW_Update.tar) to [X.X.X.X]
Warning: Permanently added 'X.X.X.X' (ECDSA) to the list of known hosts.
Transfer done.
Check running upgrade status ...
Check firmware binary signature
Uncompress and flash upgrade  - inProgress(%):11
Uncompress and flash upgrade  - inProgress(%):28
Uncompress and flash upgrade  - inProgress(%):44
Uncompress and flash upgrade  - inProgress(%):61
Uncompress and flash upgrade  - inProgress(%):78
Uncompress and flash upgrade  - inProgress(%):92
Uncompress and flash upgrade  - inProgress(%):100
Uncompress and flash upgrade  - inProgress(%):100
Uncompress and flash upgrade
Executing post post_upgrade.sh script upgrade
Upgrade done
Warning: Permanently added 'X.X.X.X' (ECDSA) to the list of known hosts.
Rebooting...
res: Y
Update:  OK
```

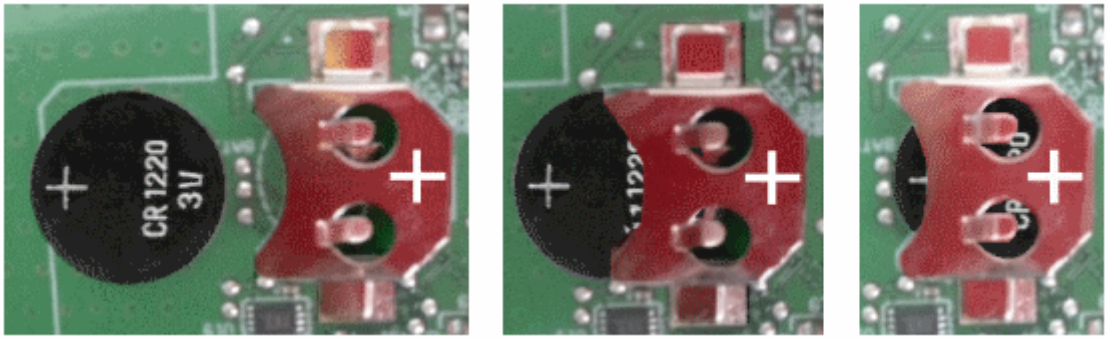
3.11 Changing the RTC battery cell

1. Access the Network Module, and then disconnect the Network cable, if needed.
2. Unscrew the Network Module and remove it from the slot.
3. Locate the RTC battery cell located on the back of the Network Module.



4. Get a new battery cell (CR1220 type).

5. Replace the battery cell, the positive mark (+) should be visible when inserting it.



6. Replace the Network Module and secure the screw, reconnect the Network cable if it was unplugged during the operation.
7. Connect the Network Module and set the date and time. For more information, see the Date & Time section.

3.12 Updating the time of the Network Module precisely and permanently (ntp server)

For an accurate and quick update of the RTC for the Network Module, we recommend implementing a NTP server as time source for the Network Module.

LANs have an internal NTP server (Domain Controller, mail servers, Outlook servers are generally time servers too) but you can use a public ntp server like pool.ntp.org (after addition of the related rules to your firewall system).

For more information, see the Date and Time section.

3.13 Synchronizing the time of the Network Module and the UPS

⚠ This section is valid only when the UPS can manage date and time (refer to the UPS user manual for confirmation).

ⓘ The Network Module use UTC time and manage the time zone and the DST.
The UPS manage only the local time.

3.13.1 Automatic time synchronization

Every day at 5 a.m.

The UPS time (local time) is synchronized with the Network Module.

If the Network Module time is lost

The Network Module and the UPS time is synchronized with the oldest time between the last know Network Module time and the UPS time.

3.13.2 Manual time synchronization

From the Network Module

On the Network Module, navigate to Settings>>>Date & Time section and update the time.

The UPS time (local time) is directly synchronized with the Network Module.

From the UPS

ⓘ When the time is updated on the UPS, it is not synchronized on the Network Module.

3.14 Changing the language of the web pages

Update the language of the web page in the Settings menu.

1. Navigate to Settings>>>My preferences>>>Language.
2. Select the language, and then press the **Save** button.

ⓘ The language of the login page is English by default or browser language when it is supported.

3.15 Resetting username and password

3.15.1 As an admin for other users

1. Navigate to Settings>>>Users.
2. Press the pen icon  to edit user information.

3. Change username and save the changes.
4. Select Reset password and choose from the following options :
    - Generate randomly
    - Enter manually
    - Force password to be changed on next login
5. Enter your own password to confirm the changes.
6. Save the changes.

3.15.2 Resetting its own password

1. Navigate to Settings>>>My preferences>>>Profile.
2. Press Change password
3. Enter your current password, the new password twice.
4. Press **Continue** to save the changes.

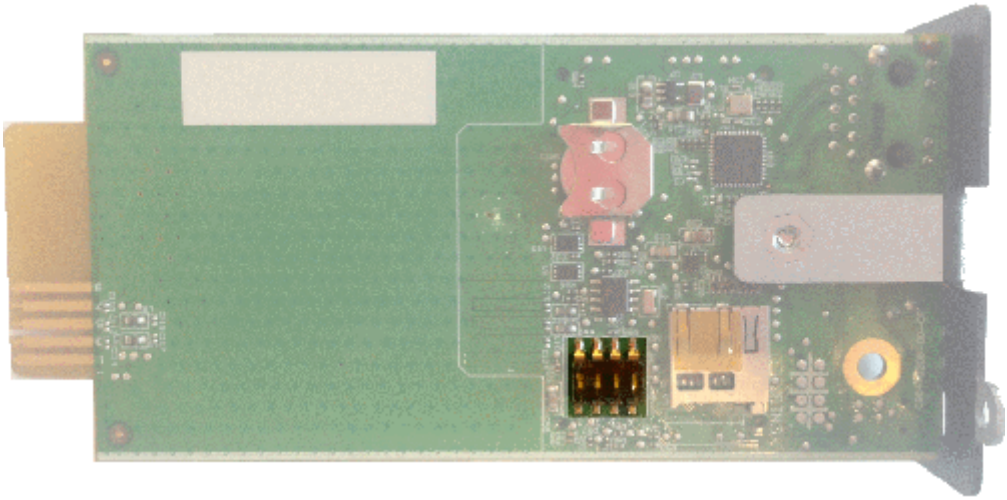
3.16 Recovering main administrator password

To recover the main administrator password, ask another administrator to initialize the password.

If it is not possible, proceed to the card sanitization:

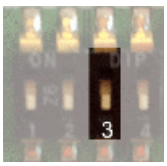
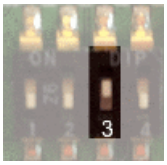
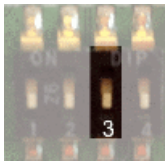
> **Below instruction will sanitize the card and blank all the data.**
> Depending on your network configuration, the Network Module may restart with a different IP address.
> Only main administrator user will remain with default login and password.
> Refresh the browser after the Network module reboot time to get access to the login page.

1. Access the Network Module, disconnect the Network cable, if needed.
2. Unscrew the Network Module and remove it from the slot.
3. Locate the SANITIZATION switch that is located on the back of the Network Module.



4. Peel off the protection :

5. Change the position of switch number 3, this change is detected during next power ON and the sanitization will be applied :

Case 1 :		
Case 2 :		

Changes of the switches 1, 2 or 4 has no effect.

6. Replace the Network Module and secure the screw, connect the Network cable, if needed.
7. Connect the Network Module by using the default credentials of the main administrator : admin/admin.
8. You will be forced to change the password accordingly to the current password strength rules.

3.17 Switching to static IP (Manual) / Changing IP address of the Network Module

Administrators can switch to static IP in the Settings menu and change the IP address of the Network Module.

1. Navigate to Settings>>>Network>>>IPV4.
2. Select Manual (Static IP).
3. Input the following information:
    - IPv4 Address
    - Subnet Mask
    - Default Gateway
4. Save the changes.

3.18 Reading product (UPS) information in a simple way

3.18.1 Web page

The product information is located in the Home page, specifically with the Details button on the top of the diagram and in the Meters menu.

3.19 Subscribing to a set of alarms for email notification

3.19.1 Example #1: subscribing only to one alarm (load unprotected)

Follow the steps below:

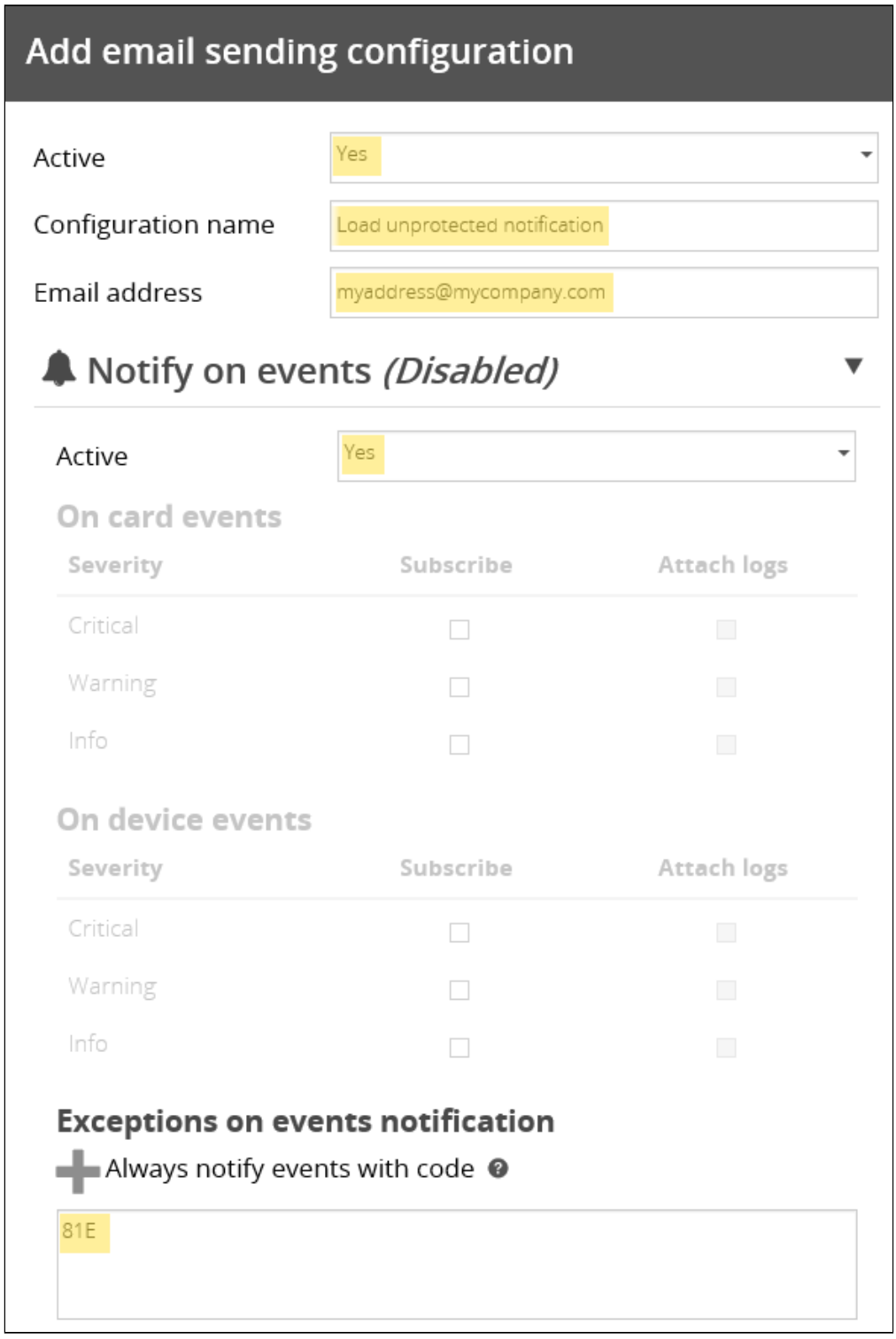
1. Navigate to Settings>>>Email>>>Email sending configuration.

2. Press the button **New** to create a new configuration.

3. Select:

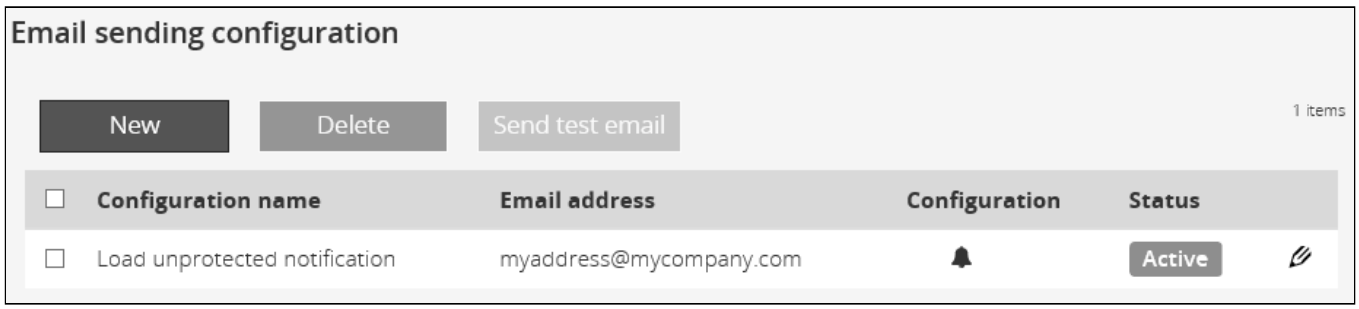
- Active: Yes
- Configuration name: Load unprotected notification
- Email address: myaddress@mycompany.com

- Notify on events: Active
- Always notify events with code: 81E (Load unprotected)



Logs will be attached by default in that example even if there is no subscription on card or device events.

4. Press **Save**, the table will show the new configuration.



3.19.2 Example #2: subscribing to all Critical alarms and some specific Warnings

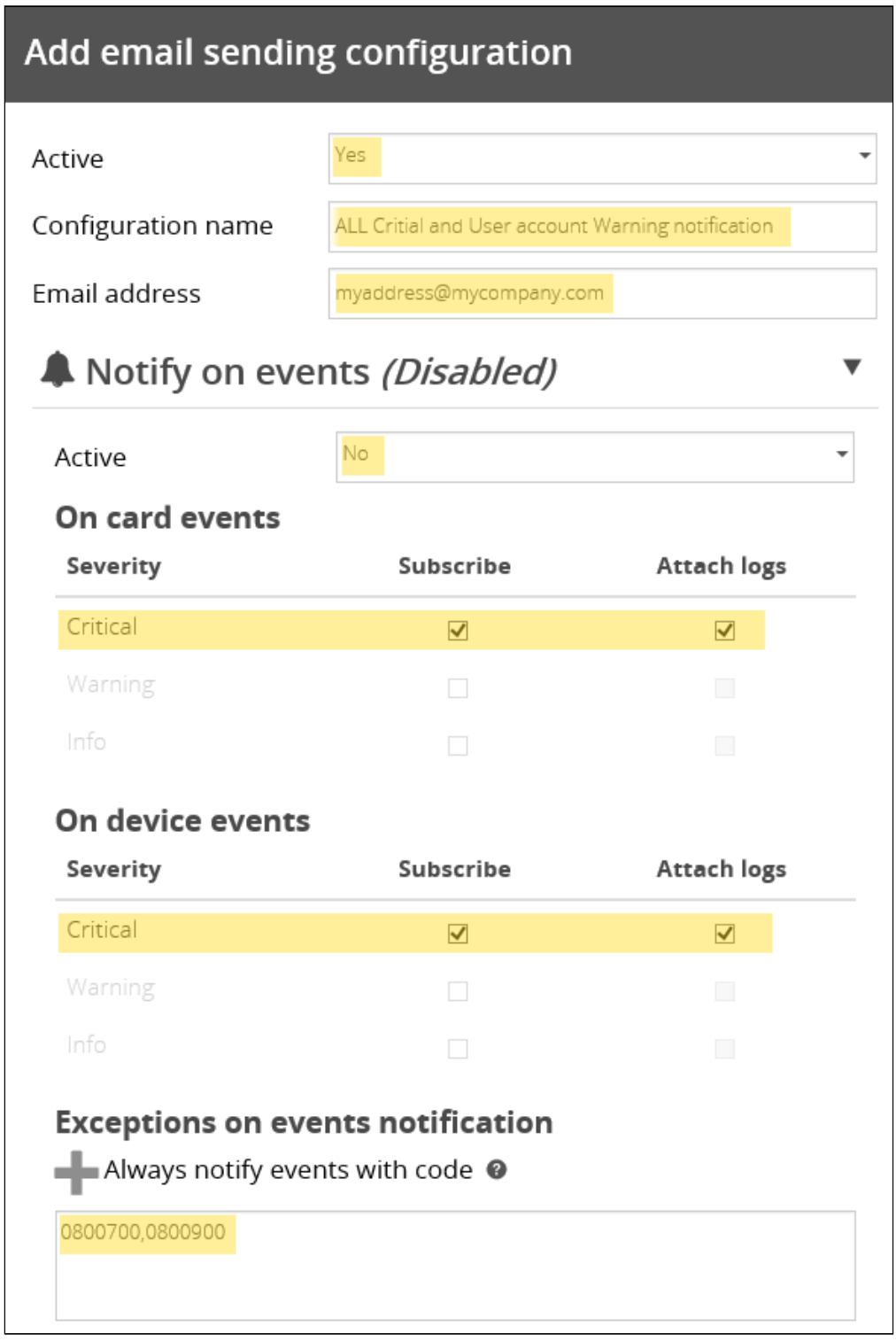
Follow the steps below:

1. Navigate to Settings>>>Email>>>Email sending configuration.

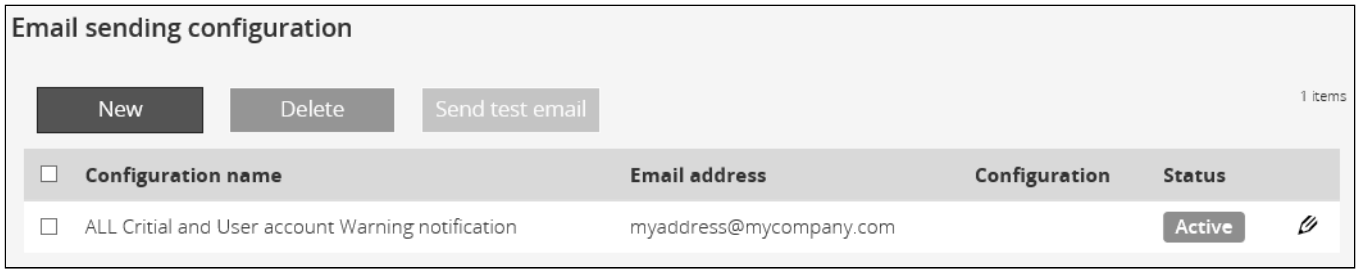
2. Press the button **New** to create a new configuration.

3. Select:

- Active: Yes
- Configuration name: ALL Critical and User account Warning notification
- Email address: myaddress@mycompany.com
- Notify on events: Active
- Subscribe to Critical card events and Critical device events
- Always notify events with code: 0800700, 0800900 (User account - password expired, User account- locked)



4. Press **Save**, the table will show the new configuration.

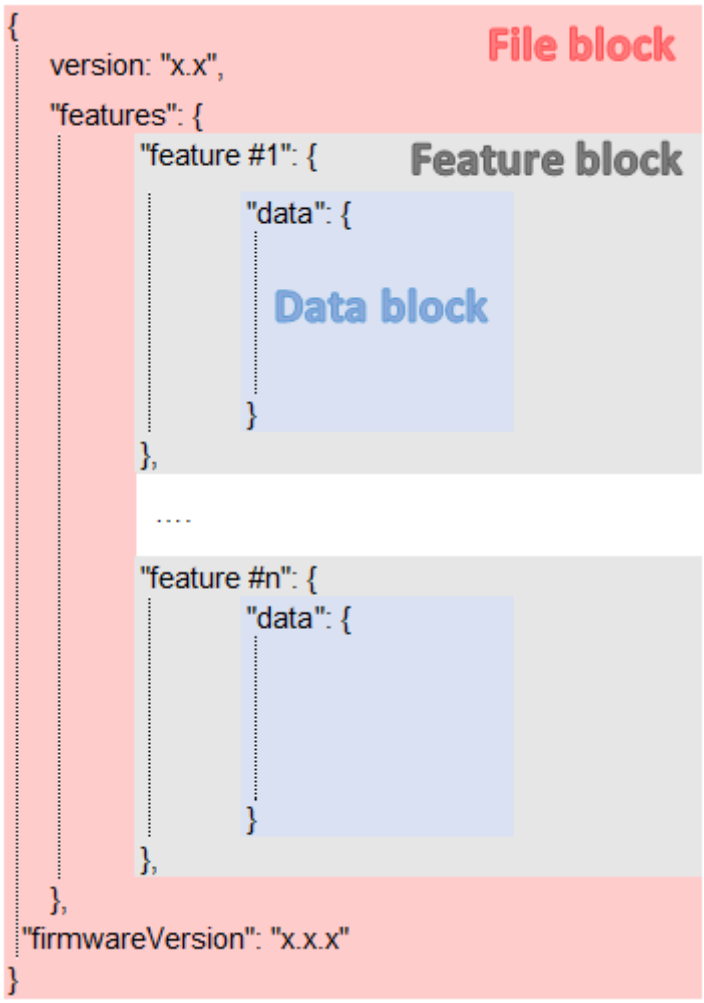


3.20 Saving/Restoring/Duplicating Network module configuration settings

3.20.1 Modifying the JSON configuration settings file

JSON file structure

The JSON file is structured into 3 blocks:

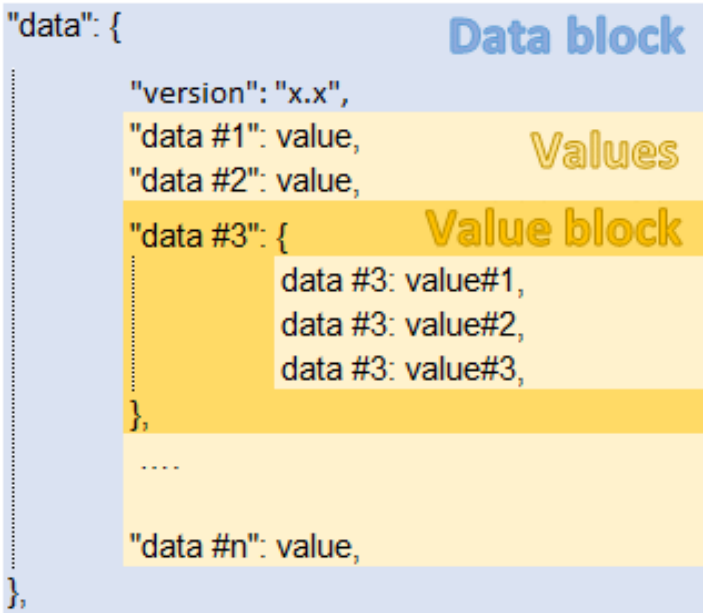


File block
: File block cannot be modified, this is the mandatory structure of the JSON file.

Feature block
: Feature block contains the full definition of a feature.

  If it is removed from the JSON file, this feature settings will not be updated/restored in the card.

Data block
: Data block contains all the feature settings values.



Data block
Data block cannot be modified, this is the mandatory structure of the JSON file.

Value block
If some values inside the Value block need to be kept, Value block structure cannot be modified, this is the mandatory structure of the JSON file.

If it is removed from the JSON file, these values will not be updated/restored.

Values
Values can be kept as is, modified or removed.

Removed values will not be updated/restored.

Sensitive data (like passwords)

JSON file structure will slightly varies if sensitive data are exported with passphrase or not.

The JSON file is saved using passphrase (preferred)

All sensitive data will have below structure:

```
"password": {
        plaintext: "null",
        cyphered: "p-twlcjoV-a8FjMjkagL6w"
},
```

When restoring the file, the corresponding setting will be updated based on the cyphered value.

The JSON file is saved **without** passphrase

All sensitive data will have below structure:

```
"password": {
        plaintext: "null",
},
```

When restoring the file, the corresponding setting will not be set.
This may lead to restoration failure if corresponding setting was not previously set with a valid value.

Modifying JSON file examples

Modifying sensitive data

To change sensitive data, plain text must be filled with the new value **and the Cyphered entry (if existing) must be removed:**

```
"password": {
        plaintext: "New password",
},
```

Adding local users

Original file: • **1 x predefined account (main administrator)** • **1 x account**	**Modified file:** • **1 x predefined account (main administrator)** • **2 x accounts**

```
PredefinedAccounts: [
{
        credentials: {
                enabled: true,
                username: "admin",
                passwordExpired: false,
                locked: false,
                profile: "administrators",
                password: {Plaintext: "",Cyphered:"xxxxx"},
        },
        vCard: {
                fullName: "xxxxr",
                email: "xxxxx",
                phone: "xxxxx",
                organization: "xxxxx"
        },
        preferences: {
                notifyByMail: xxxx,
                licenseAgreed: xxxx,
                language: "xx",
                dateFormat: "xxxx",
                timeFormat: x,
                temperatureUnit: x
        }
}
        ],
```

```
accounts: [
        {
        credentials: {
                enabled: xxxx,
                username: "xxxxx",
                passwordExpired: xxxx,
                locked: xxxx,
                profile: "xxxx",
                password: {Plaintext: "",Cyphered:"xxxxxxxxxx"},
                },
        vCard: {
                fullName: "xxxxx",
                email: "xxxxx",
                phone: "xxxxx",
                organization: "xxxxx"
                },
        preferences: {
                notifyByMail: xxxx,
                licenseAgreed: xxxx,
                language: "xx",
                dateFormat: "xxxxx",
                timeFormat: x,
                temperatureUnit: x
                }
        }
]
```

```
PredefinedAccounts: [
{
        credentials: {
                enabled: true,
                username: "admin",
                passwordExpired: false,
                locked: false,
                profile: "administrators",
                password: {Plaintext: "",Cyphered:"xxxxx"},
        },
        vCard: {
                fullName: "xxxxr",
                email: "xxxxx",
                phone: "xxxxx",
                organization: "xxxxx"
        },
        preferences: {
                notifyByMail: xxxx,
                licenseAgreed: xxxx,
                language: "xx",
                dateFormat: "xxxx",
                timeFormat: x,
                temperatureUnit: x
        }
}
        ],
```

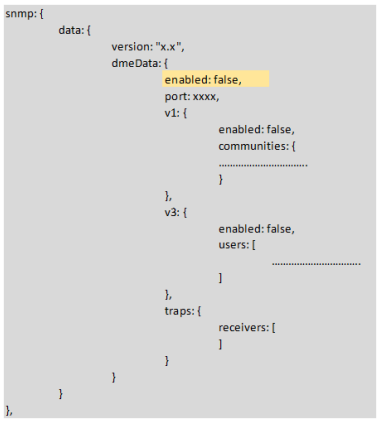
Original file: • **1 x predefined account (main administrator)** • **1 x account**	**Modified file:** • **1 x predefined account (main administrator)** • **2 x accounts**

	accounts: [
	{
	credentials: {
	enabled: xxxx,
	username: "xxxxx",
	passwordExpired: xxxx,
	locked: xxxx,
	profile: "xxxx",
	password: {Plaintext: "",Cyphered:"xxxxxxxxxx"},
	},
	vCard: {
	fullName: "xxxxx",
	email: "xxxxx",
	phone: "xxxxx",
	organization: "xxxxx"
	},
	preferences: {
	notifyByMail: xxxx,
	licenseAgreed: xxxx,
	language: "xx",
	dateFormat: "xxxxx",
	timeFormat: x,
	temperatureUnit: x
	}
	},
	{
	credentials: {
	enabled: xxxx,
	username: "yyyyy",
	passwordExpired: xxxx,
	locked: xxxx,
	profile: "xxxx",
	password: {Plaintext: "yyyyy",Cyphered:""},
	},
	vCard: {
	fullName: "yyyyy",
	email: "yyyyy",
	phone: "yyyyy",
	organization: "xxxxx"
	},
	preferences: {
	notifyByMail: xxxx,
	licenseAgreed: xxxx,
	language: "xx",
	dateFormat: "xxxxx",
	timeFormat: x,
	temperatureUnit: x
	}
	}
	]

Modifying SNMP settings

Original file:

- **SNMP disabled**



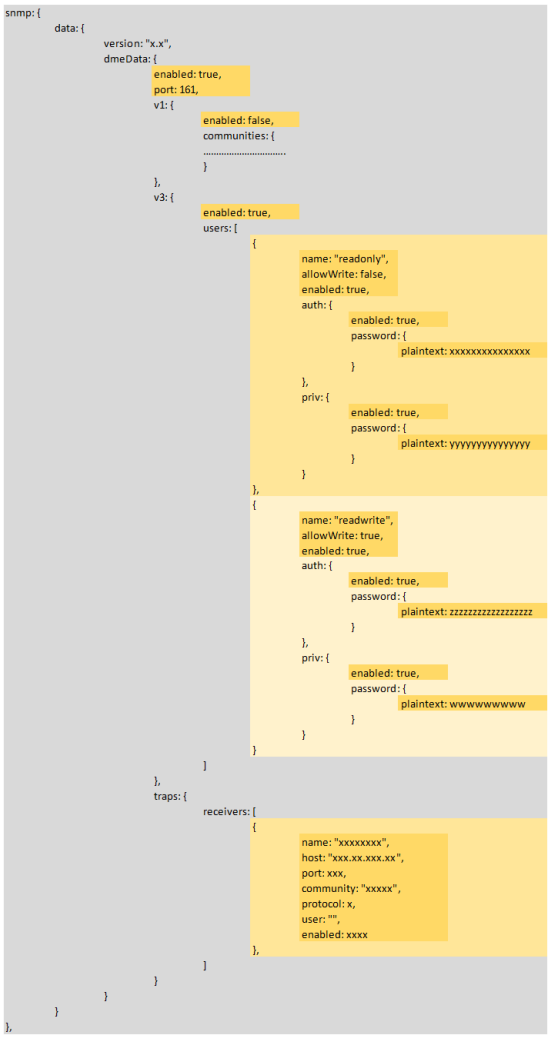
Modified file:

- **SNMP enabled on port 161**
- **SNMPv1 disabled**
- **SNMPv3 enabled**
- **2 x accounts**

  1 x read only user (enabled) with Auth-Priv security level and passwords

  1x read write user (enabled) with Auth-Priv security level and passwords

- **1 x active trap**



Making a partial update/restoration

Example: Updating/Restoring only LDAP settings
If you restore below JSON content, only LDAP settings will be updated/restored, everything else will remain unchanged.

```
{
        "version": "x.x",
        "features": {
                "ldap": {
                        "data": {
                        "version": "x.x",
                        "certificateData": [],
                        "dmeData": {
                                "enabled": true,
                                "baseAccess": {
                                        "security": {"ssl": 1,"verifyTlsCert": false},
                                        "primary": {"name": "Primary","hostname":
"xxxxxxxxx","port": xxxx},
                                        "secondary": {"name": "xxxxxx","hostname":
"xxxxxx","port": xxxx},
                                        "credentials": {
                                                "anonymousSearchBind": false,
                                                "searchUserDN":

"CN=xxxx,OU=xxxx,OU=xxxx,OU=xxxx,DC=xxxx,DC=xxxx",
                                                "password": {"plaintext": null}},
                                        "searchBase": {"searchBaseDN": "DC=xxx,DC=xxx,DC=xxx"
}
                                        },
                                "requestParameters": {
                                        "userBaseDN": "OU=xxxx,DC=xxxx",
                                        "userNameAttribute": "xxxx",
                                        "uidAttribute":"objectSid:x-x-x-xx-xxxxxxxxxx-
xxxxxxxxxx-xxxxxxxxxx",
                                        "groupBaseDN": "OU=xxxx,DC=xxxx",
                                        "groupNameAttribute": "xx",
                                        "gidAttribute":"objectSid:x-x-x-xx-xxxxxxxxxx-
xxxxxxxxxx-xxxxxxxxxx"
                                        },
                                "profileMapping": [
                                        { "remoteGroup": "xxxxxxxxxxxxxx","profile": 1},
                                        { "remoteGroup": "xxxxxxxxxxxxxx","profile": 2},
                                        { "remoteGroup": "","profile": 0},
                                        { "remoteGroup": "","profile": 0},
                                        { "remoteGroup": "","profile": 0}
                                        ]
                                        }
                                }
                        },
                },
"firmwareVersion": "x.x.x"
}
```


Non-intuitive data values in the JSON file

Features	Data	Values example
Account service	preferences>>>language	de: Deutsh en: English es: Español fr: Français it: Italiano ja: 日本語 zh_Hans: 简体中文 zh_Hant:繁體中文
	preferences>>>dateFormat	Y-m-d: YYYY-MM-DD d-m-Y: DD-MM-YYYY d.m.Y: DD.MM.YYYY d/m/Y: DD/MM/YYYY m/d/Y: MM/DD/YYYY d m Y: DD MM YYYY
	preferences>>>timeFormat	1: 24h 0: 12h
	preferences>>>temperatureUnit	1: °C 2: °F
Card	-	-
Date	timeZone	"Europe/Paris","Africa/Johannesburg","America/New_York","Asia/Shanghai" *Refer to the Web interface for the full list.*
email	periodicReport>>>periodicity	Every day Every week Every month
	periodicReport>>>startTime	timestamp (unix)
LDAP	baseAccess>>>security>>>ssl	1: None 2: Start TLS 3: SSL

	baseAccess>>>profileMapping>>>profile	administrators viewers operators
Measure	-	-
Modbus	rtu>>>configuration>>>baudrate	1: 1200pbs 2: 2400bps 3: 4800bps 4: 9600bps 5: 19200bps 6: 38400bps 7: 57600bps 8: 115200bps
	rtu>>>configuration>>>parity	1: None 2: Even 3: Odd
	rtu>>>configuration>>>stopBits	1: 1 Stop bit 2: 2 Stop bits
	mapping>>>configurations>>>transport	1: RTU 2: TCP
	mapping>>>configurations>>>map	network_card: Card System Information modbus_ms: Eaton ModbusMS compatible
	mapping>>>configurations>>>transportFilter	*: Access to all xx.xxx.xx.xx;yy.yyy.yy.yy;...: Access to a list of IP address
	mapping>>>configurations>>>deviceID	1 to 247
	mapping>>>configurations>>>access	0: None 1: Read only 3: Read/Write
	mapping>>>configurations>>>illegalReadBehavior	1: Return exception 2: return zeros
MQTT	-	-

Power outage policy	id	Internal id, please don't modify it. Power outage policy configuration cannot be duplicated without manual configuration through the Web interface.
Remote user	preferences>>>language	de: Deutsh en: English es: Español fr: Français it: Italiano ja: 日本語 zh_Hans: 简体中文 zh_Hant:繁體中文
	preferences>>>dateFormat	Y-m-d: YYYY-MM-DD d-m-Y: DD-MM-YYYY d.m.Y: DD.MM.YYYY d/m/Y: DD/MM/YYYY m/d/Y: MM/DD/YYYY d m Y: DD MM YYYY
	preferences>>>timeFormat	1: 24h 0: 12h
	preferences>>>temperatureUnit	1: °C 2: °F
Schedule	scheduler	Scheduler configuration cannot be duplicated without manual configuration through the Web interface.
	recurrence	0: once 1: every day 2: every week
	shutdownTimeStamp	timestamp (unix)
	restartTimeStamp	timestamp (unix)
SMTP	-	-
SNMP	traps>>>receivers>>>protocol	1: SNMP v1 3: SNMP v2

	traps>>>receivers>>>user	User configuration cannot be duplicated without manual configuration through the Web interface.
Syslog	servers>>>protocol	1: UDP 2: TCP
	servers>>>tcpframing	1: TRADITIONAL 2: OCTET_COUNTING
Web server	-	-

3.20.2 Saving/Restoring/Duplicating settings through the CLI

Navigate to Information>>>CLI>>>save_configuration | restore_configuration section to get example on how to save and restore settings through the CLI.

3.20.3 Saving/Restoring/Duplicating settings through the Web interface

Navigate to Card>>>Administration section to get information on how to save and restore settings through the Web interface.

4 Securing the Network Management Module

4.1 Cybersecurity considerations for electrical distribution systems

4.1.1 Purpose

The purpose of this section is to provide high-level guidance to help customers across industries and applications apply Eaton solutions for power management of electrical systems in accordance with current cybersecurity standards.
This document is intended to provide an overview of key security features and practices to consider in order to meet industry recommended standards and best practices.

4.1.2 Introduction

Every day, cyber-attacks against government and commercial computer networks number in the millions. According to U.S. Cyber Command, Pentagon systems are probed 250,000 times per hour. Similar attacks are becoming more prevalent on other kinds of information-based smart networks as well, such as those that operate buildings and utility systems. Whether the objective is to steal intellectual property or halt operations, the tools and the techniques used for unauthorized network access are increasingly sophisticated.

4.1.3 Connectivity—why do we need to address cybersecurity for industrial control systems (ICS)?

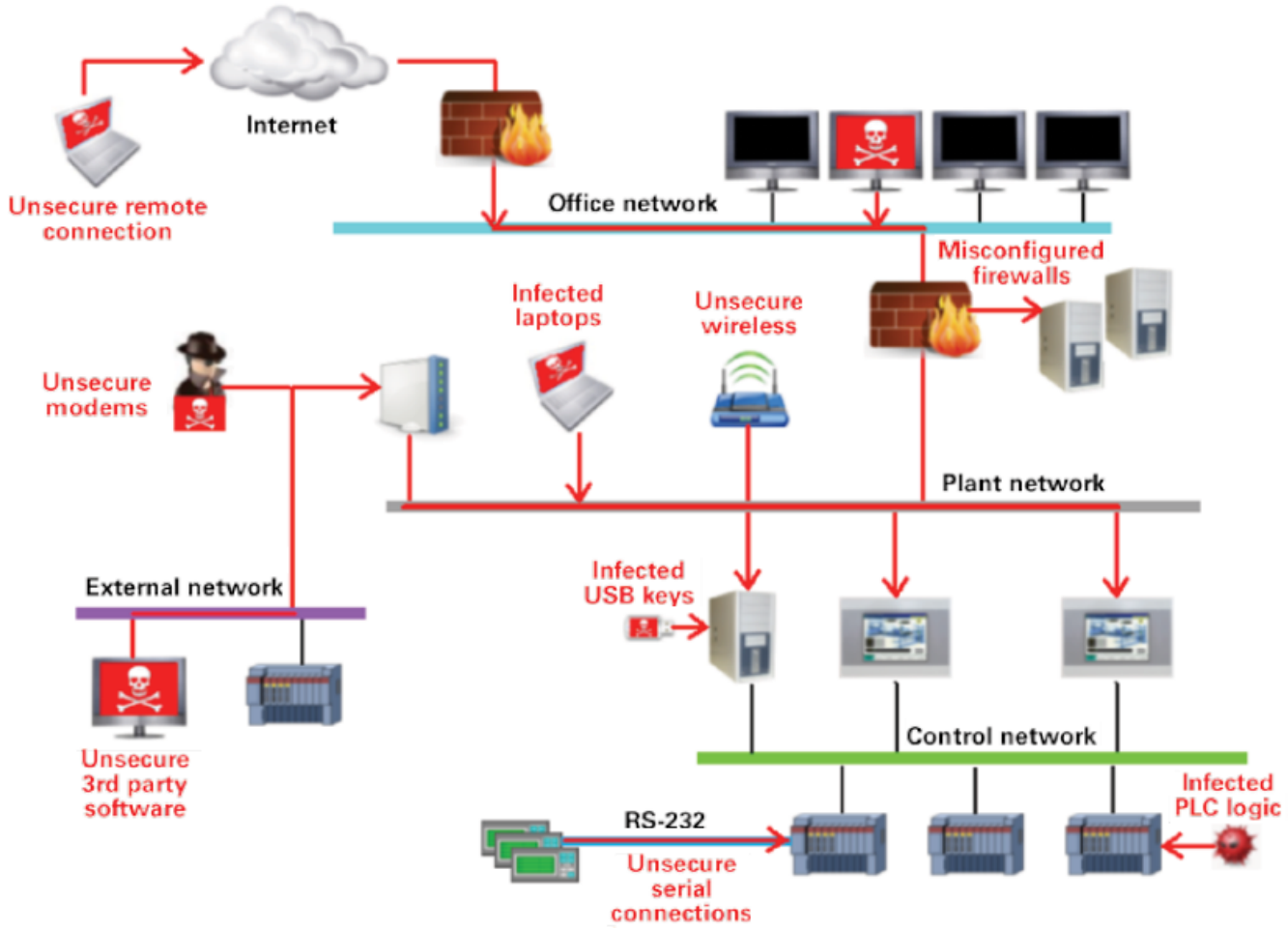
There is increasing concern regarding cybersecurity across industries where companies are steadily integrating field devices into enterprise-wide information systems. This occurs in discrete manufacturing and process industrial environments, a wide range of general and specific purpose commercial buildings, and even utility networks. Traditionally, electrical systems were controlled through serial devices connected to computers via dedicated transceivers with proprietary protocols. In contrast, today's control systems are increasingly connected to larger enterprise networks, which can expose these systems to similar vulnerabilities that are typically found in computer systems. The differences between information technology (IT) and ICS networks can be summarized as follows:

- The main focus of the IT network is to ensure the **confidentiality** and the **integrity** of the data using rigorous access control and data encryption
- The main focus of the ICS network is **safety**, **availability**, and **integrity** of data
- Enterprise security protects the servers' data from attack
- Control system security protects the facility's ability to safely and securely operate, regardless of what may befall the rest of the network

4.1.4 Cybersecurity threat vectors

Cybersecurity threat vectors are paths or tools that an entity can use to gain access to a device or a control network in order to deliver a malicious attack. Figure below shows examples of attack vectors on a network that might otherwise seem secure.

Paths to the control network



The paths in above figure include:

- External users accessing the network through the Internet
- Misconfigured firewalls
- Unsecure wireless routers and wired modems
- Infected laptops located elsewhere that can access the network behind the firewall
- Infected USB keys and PLC logic programs
- Unsecure RS-232 serial links

The most common malicious attacks come in the following forms:

- Virus—a software program that spreads from one device to another, affecting operation
- Trojan horse—a malicious device program that hides inside other programs and provides access to that device
- Worm—a device program that spreads without user interaction and affects the stability and performance of the ICS network
- Spyware—a device program that changes the configuration of a device

4.1.5 Defense in depth

While there are differences between traditional IT systems and ICS, the fundamental concept of “defense in depth” is applicable to both. Defense in depth is a strategy of integrating technology, people, and operations capabilities to establish variable barriers across multiple layers of an organization. These barriers include electronic countermeasures such as firewalls, intrusion detection software/components, and antivirus software, coupled with physical protection policies and training. Fundamentally, the barriers are intended to reduce the probability of attacks on the network and provide mechanisms to detect “intruders.”

4.1.6 Designing for the threat vectors

Firewalls

Firewalls provide the capability to add stringent and multifaceted rules for communication between various network segments and zones in an ICS network. They can be configured to block data from certain segments, while allowing the relevant and necessary data through. A thorough understanding of the devices, applications, and services that are in a network will guide the appropriate deployment and configuration of firewalls in a network. Typical types of firewalls that can be deployed in a network include:

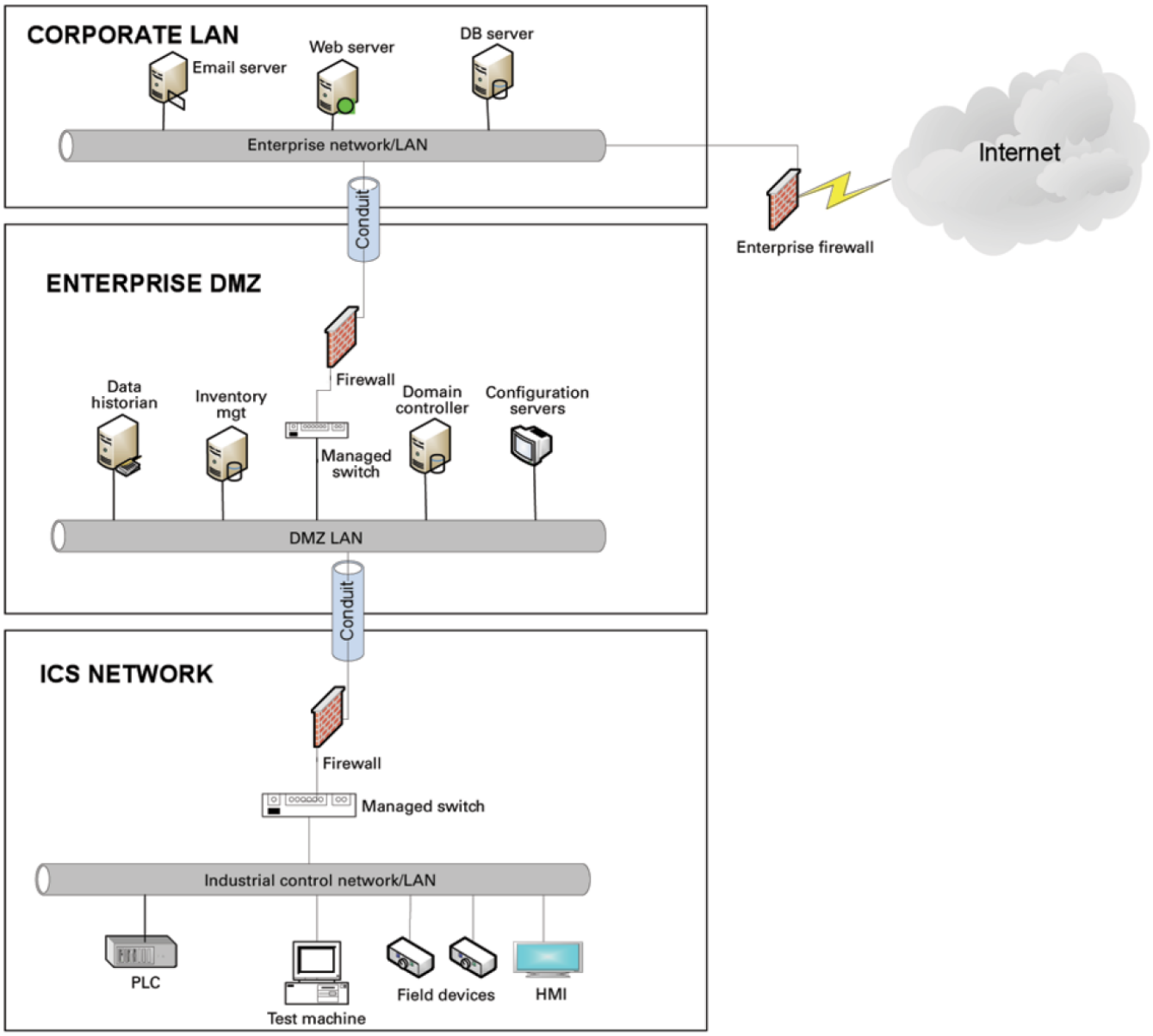
- **Packet filter or boundary firewalls that work on the network layer**
  These firewalls mainly operate at the network layer, using pre-established rules based on port numbers and protocols to analyze the packets going into or out of a separated network.
  These firewalls either permit or deny passage based on these rules.
- **Host firewalls**
  These firewalls are software firewall solutions that protect ports and services on devices. Host firewalls can apply rules that track, allow, or deny incoming and outgoing traffic on the device and are mainly found on mobile devices, laptops, and desktops that can be easily connected to an ICS.

- **Application-level proxy firewalls**
  These firewalls are highly secure firewall protection methods that hide and protect individual devices and computers in a control network. These firewalls communicate at the application layer and can provide better inspection capabilities. Because they collect extensive log data, application-level proxy firewalls can negatively impact the performance of an ICS network.
- **Stateful inspection firewalls**
  These firewalls work at the network, session, and application layers of the open system interconnection (OSI). Stateful inspection firewalls are more secure than packet filter firewalls because they only allow packets belonging to allowed sessions.
  These firewalls can authenticate users when a session is established and analyze a packet to determine whether they contain the expected payload type or enforce constraints at the application layer.
- **SCADA hardware firewalls**
  These are hardware-based firewalls that provide defense for an ICS based on observing abnormal behavior on a device within the control network. For example, if an operator station computer suddenly attempts to program a PLC, this activity could be blocked and an alarm could be raised to prevent serious risk to the system.

Demilitarized zones (DMZ)

Network segmentation is a key consideration in establishing secure control networks. Firewalls should be used to create DMZ by grouping critical components and isolating them from the traditional business IT network. A three-tier architecture should be employed at a minimum, with a DMZ between the organization’s core network and an isolated control system’s network as shown in below figure.

Three-tier architecture for a secure control network



Above figure shows that the control networks are divided into layers or zones based on control functions, which are then connected by conduits (connections between the zones) that provide security controls to:

- Control access to zones
- Resist denial of services (DOS) attacks or the transfer of malware
- Shield other network systems
- Protect the integrity and the confidentiality of network traffic

Beyond network segmentation, access control (both physical and logical) should be defined and implemented.

The key consideration when designing access control is defining the **required** interactions both within a given zone and between zones. These interactions should be mapped out clearly and prioritized based on need. It is important to realize that every hole poked in a firewall and each non-essential functionality that provides access or creates additional connectivity increases potential exposure to attacks. A system then becomes only as secure as the devices connecting to it.

If mapped correctly, the potential adverse impact to control system reliability and functionality should be negligible. However, this element introduces additional costs (in terms of firewall and other network infrastructure) and complexity to the environment.

Intrusion detection and prevention systems (IDPS)

These are systems that are primarily focused on identifying possible incidents in an ICS network, logging the information about them, attempting to stop them, and reporting them to ICS security administrators.

Because these systems are critical in an ICS network, they are regular targets for attacks and securing them is extremely important.

The type of IDPS technology deployed will vary with the type of events that need to be monitored.

There are four classes of IDPS technology:

- Network-based IDPS monitors network traffic for particular ICS network segments or devices and analyzes the network and application protocol activity to identify suspicious activity
- Wireless IDPS monitors and analyzes wireless network traffic to identify suspicious activity involving the ICS wireless network protocol
- Network behavior analysis IDPS examines ICS network traffic to identify threats that generate unusual traffic flows such as DOS attacks
- Host-based IDPS monitors the characteristics and the events occurring within a single ICS network host for suspicious activity

4.1.7 Policies, procedures, standards, and guidelines

For the defense in depth strategy to succeed, there must be well-documented and continuously reviewed policies, procedures, standards, and guidelines.

- **Policies** provide procedures or actions that must be carried out to meet objectives and to address the who, what, and why
- **Procedures** provide detailed steps to follow for operations and to address the how, where, and when
- **Standards** typically refer to specific hardware and software, and specify uniform use and implementation of specific technologies or parameters
- **Guidelines** provide recommendations on a method to implement the policies, procedures, and standards

Understanding an ICS network

Creating an inventory of all the devices, applications, and services that are hosted in a network can establish an initial baseline for what to monitor. Once those components are identified and understood, control, ownership, and operational consideration can be developed.

Log and event management

It is important to understand what is happening within the network from both a performance and security perspective. This is especially true in a control systems environment.

Log and event management entails monitoring infrastructure components such as routers, firewalls, and IDS/IPS, as well as host assets. Security Information and Event Management (SIEM) systems can collect events from various sources and provide correlation and alerts.

Generating and collecting events, or even implementing a SIEM is not sufficient by itself. Many organizations have SIEM solutions, but alerts go unwatched or unnoticed.

Monitoring includes both the capability to monitor environments and the capacity to perform the monitoring. Capability relates to the
design and the architecture of the environment. Has it been built in a manner that takes into consideration the ability to monitor? Capacity speaks to the resources (personnel, tools, expertise) needed to perform meaningful interpretation of the information and initiate timely and appropriate action.

Through monitoring, the organization can identify issues such as suspicious or malicious activities. Awareness can be raised when new (potentially unauthorized) devices appear in the environment. Careful consideration should be taken into account to ensure that log and event management does not adversely impact the functionality or the reliability of the control system devices.

Security policy and procedures

It is important to identify “asset owners,” and to develop policies and procedures for a cybersecurity program. These policies need
to be practical and enforceable in order to be effective. Policies should also address access related issues, such as physical access, contractors, and vendors.

Existing (traditional) IT standards and policies may not apply (or have not been considered) for control systems. A gap analysis should be performed to determine which components are not covered (or not adequately covered) by existing policies. Relationships with existing policies and standards should be explicitly identified and new or supporting policies should be developed. It is important that industrial control system administrators have proper authorizations and full support of their management to implement policies that will help secure the ICS network.

ICS hardening

The goal for system hardening is to reduce as many security risks as possible by securely configuring ICS networks. The idea is to
establish configurations based on what is required and eliminate unnecessary services and applications that could potentially provide another possible entry point to an intruder.

Minimum security baselines should be established for the various platforms and products deployed (operating system, application, and infrastructure elements such as drives, meters, HMI devices). The following actions should be implemented where applicable:

- Disable unnecessary services
- Disable anonymous FTP
- Do not use clear text protocols (e.g., use SSH v2 instead of Telnet)
- Install only required packages/applications/features
- Deploy antivirus solutions (where possible)
- Disable or otherwise control use of USB devices
- Establish a warning banner
- Change default passwords (e.g., SNMP)

It may be easier to implement these actions on devices for which you control the base operating system platform. However, several
of the items listed above can be configured from the product specific configuration options.

Changes such as these could potentially impact the functionality of a control system device. Extensive testing needs to be conducted before deployment to minimize this impact.

Continuous assessment and security training

It is critical that ICS network administrators and regular users be properly trained to ensure the security of the ICS and the safety of
the people who operate and depend on it.

Ongoing vulnerability assessments are critical to identify issues and understand the effectiveness of other defensible network elements.

Assessments should include testing and validating the following:

- Monitoring capabilities and alerts are triggered and responded to as expected
- Device configuration of services and applications
- Expected connectivity within and between zones
- Existence of previously unknown vulnerabilities in the environment
- Effectiveness of patching

A program should be established for performing assessments.
The actual assessment should be performed by a qualified resource, which can be an in-house or third-party organization. Regardless of who performs the assessments, in-house resources need to be involved in the planning, scoping, and supporting of assessment activities and must be appropriately trained to do so.

Assessments should be conducted according to a methodology that is clearly defined to address:

- Physical security

- People and processes
- Network security
- Host security
- Applications security (both internally developed and commercially off-the-shelf (COTS))

Patch management planning and procedures

A patching and vulnerability management process should be established based on the timely awareness of issues and appropriate action. This process should take all of the elements that make up the control system environment into consideration.

Information resources should be identified for vulnerability and advisory information for the various components in the environment. These should include vendor-specific sources as well as other public or commercial services that provide vulnerability advisory information. For example, the National Vulnerability Database (NVD) provides information related to vulnerabilities identified in general IT components, while the Industrial Control Systems Cyber Emergency Response Team (ICS-CERT) publishes advisories specific to control systems.

A regular patch deployment schedule should be established for each component in the environment. Depending on the component, this could range from a monthly schedule to an as-needed deployment, depending on the historical frequency of patch or vulnerability related issues for the component or the vendor. Additionally, out-of-band or emergency patch management needs to be
considered and qualifications need to be defined.

Vulnerability information and advisories should be reviewed regularly and assessments should be performed to determine the relative severity and urgency of issues.

Elements of the process should also include the preparation, scheduling, and change controls; testing and rollback procedures;
and pre-deployment notification to stakeholders that includes scope, expectations, and reporting. Testing is a significant element, as
the effect of the patch application needs to be clearly understood; unintended or unexpected impacts to a control system component influence the decision to deploy a patch. In the event that it is determined that a patch cannot be safely deployed but the severity of the issue represents a significant concern, compensating controls should be investigated.

4.1.8 Conclusion

To protect important assets, all organizations must take cybersecurity threats seriously and meet them proactively with a system-wide defensive approach specific to organizational needs.

There is no protection method that is completely secure. A defense mechanism that is effective today may not be effective tomorrow– the ways and means of cyber-attacks constantly change. It is critical ICS administrators remain aware of changes in cybersecurity and continue to work to prevent any potential vulnerabilities in the systems they manage.

4.1.9 Terms and definitions

DMZ	A demilitarized zone is a logical or physical sub network that interfaces an organization’s external services to a larger, untrusted network and providing an additional layer of security.
Encryption	The process of transforming plain or clear text using an algorithm to make it unreadable to anyone except those possessing special knowledge.
ICS	A device or set of device that manage, command, direct, or regulate the behavior of other devices or systems.
Protocol	A set of standard rules for data representation, signaling, authentication, and error detection required to send information over a communications channel

4.1.10 Acronyms

COTS	Commercially Off-the-Shelf
DMZ	Demilitarized Zone
DOS	Denial of Service
FTP	File Transfer Protocol
HMI	Human Machine Interface
ICS	Industrial Control Systems
ICS-CERT	Industrial Control Systems - Cyber Emergency Response Team
IDPS	Intrusion Detection and Prevention Systems
IDS	Intrusion Detection Systems
IPS	Intrusion Prevention Systems
IT	Information Technology
NVD	National Vulnerability Database
OSI	Open System Interconnection
PLC	Programmable Logic Controller
SCADA	Supervisory Control and Data Acquisition
SNMP	Simple Network Management Protocol
SSH	Secure Shell
SIEM	Security Information and Event Management
USB	Universal Serial Bus

4.1.11 References

[1] Recommended Practice: Improving Industrial Control Systems Cybersecurity with Defense-In-Depth Strategies, October 2009
https://ics-cert.us-cert.gov/sites/default/files/FactSheets/NCCIC%20ICS_FactSheet_Defense_in_Depth_Strategies_S508C.pdf
[2] NIST.SP.800-82 Guide to Industrial Control Systems (ICS) Security, June 2011
http://csrc.nist.gov/publications/nistpubs/800-82/SP800-82-final.pdf
[3] NIST.SP.800-94 Guide to Intrusion Detection and Prevention Systems (IDPS), Feb 2007
http://csrc.nist.gov/publications/nistpubs/800-94/SP800-94.pdf
[4] Common Cybersecurity Vulnerabilities in Industrial Control Systems, May 2011
http://ics-cert.uscert.gov/sites/default/files/recommended_practices/
DHS_Common_Cybersecurity_Vulnerabilities_ICS_2010.pdf
[5] The Tao of Network Security Monitoring, 2005 Richard Bejtlich

4.2 Cybersecurity recommended secure hardening guidelines

4.2.1 Introduction

This Network module has been designed with Cybersecurity as an important consideration. Number of Cybersecurity features are now offered in the product which if implemented as per the recommendations in this section would minimize Cybersecurity risk to the Network module. This section “secure configuration” or “hardening” guidelines provide information to the users to securely deploy and maintain their product to adequately minimize the cybersecurity risks to their system.

Eaton is committed to minimizing the Cybersecurity risk in its products and deploys cybersecurity best practices and latest cybersecurity technologies in its products and solutions; making them more secure, reliable and competitive for our customers. Eaton also offers Cybersecurity Best Practices whitepapers to its customers that can be referenced at www.eaton.com/cybersecurity

4.2.2 Secure configuration guidelines

Asset identification and Inventory

Keeping track of all the devices in the system is a pre-requisite for effective management of Cybersecurity of a system. Ensure you maintain an inventory of all the components in your system in a manner in which you uniquely identify each component. To facilitate this Network module supports the following identifying information - manufacturer, type, serial number, f/w version number, and location.

Network Module identification and its firmware information

It can be retrieved by navigating to *Card>>>System information*.

Identification

- System name
- Product
- Physical name
- Vendor
- UUID
- Part number
- Serial number
- Hardware version
- Location
- Contact

Firmware information

- Firmware version
- Firmware SHA
- Firmware date
- Firmware installation date
- Firmware activation date
- Bootloader version

The **COPY TO CLIPBOARD** button will copy the information to the clipboard.

Communication settings

It can be retrieved by navigating to *Settings>>>Network*

LAN

- Link status
- MAC address
- Configuration

IPV4

- Status
- Mode
- Address
- Netmask
- Gateway

Domain

- Mode
- FQDN
- Primary DNS
- Secondary DNS

IPV6

- Status
- Mode
- Addresses

UPS details

It can be retrieved by navigating to *Home>>>Details*

Details

- Name
- Model
- P/N
- S/N
- Location
- FW version

The **COPY TO CLIPBOARD** button will copy the information to the clipboard.

Physical Protection

Industrial Control Protocols don't offer cryptographic protections at protocol level, at physical ports and at controller mode switches leaving them exposed to Cybersecurity risk. Physical security is an important layer of defense in such cases. Network module is designed with the consideration that it would be deployed and operated in a physically secure location.

- Physical access to cabinets and/or enclosures containing Network module and the associated system should be restricted, monitored and logged at all times.
- Physical access to the communication lines should be restricted to prevent any attempts of wiretapping, sabotage. It's a best practice to use metal conduits for the communication lines running between one cabinet to another cabinet.
- Attacker with unauthorized physical access to the device could cause serious disruption of the device functionality. A combination of physical access controls to the location should be used, such as locks, card readers, and/or guards etc.
- Network module supports the following physical access ports, controller mode switches and USB ports: RJ45, USB A, USB Micro-B. Access to them need to be restricted.
- Do not connect unauthorized USB device or SD card for any operation (e.g. Firmware upgrade, Configuration change and Boot application change).
- Before connecting any portable device through USB or SD card slot, scan the device for malwares and virus.

Authorization and Access Control

It is extremely important to securely configure the logical access mechanisms provided in Network module to safeguard the device from unauthorized access. Eaton recommends that the available access control mechanisms be used properly to ensure that access to the system is restricted to legitimate users only. And, such users are restricted to only the privilege levels necessary to complete their job roles/functions.

- Ensure default credentials are changed upon first login. Network module should not be commissioned for production with Default credentials; it's a serious Cybersecurity flaw as the default credentials are published in the manuals.
- No password sharing – Make sure each user gets his/her own password for that desired functionality vs. sharing the passwords. Security monitoring features of Network module are created with the view of each user having his/her own unique password. Security controls will be weakened as soon as the users start sharing the password.

- Restrict administrative privileges - Threat actors are increasingly focused on gaining control of legitimate credentials, especially those associated with highly privileged accounts. Limit privileges to only those needed for a user's duties.
- Perform periodic account maintenance (remove unused accounts).
- Change passwords and other system access credentials whenever there is a personnel change.
- Use client certificates along with username and password as additional security measure.

Description of the User management in the Network Module:

- User and profiles management: (Navigate to Settings>>>Users)

  Add users
  Remove users
  Edit users

- Password/Account/Session management: (Navigate to Settings>>>Users)

  Password strength rules – Minimum length/Minimum upper case/Minimum lower case/Minimum digit/Special character
  Account expiration – Number of days before the account expiration/Number of tries before blocking the account
  Session expiration – No activity timeout/Session lease time

  See "Default settings parameters" in the embedded help for (recommended) default values.
  Additionally, it is possible to enable account expiration to force users renew their password periodically.

- Default credentials: admin/admin

  The change of the default "admin" password is enforced at first connection.

  It is also recommended to change the default "admin" user name through the *Settings>>>Users* page.
  Follow embedded help for instructions on how to edit a user account.

- Server and client certificate configuration: (Navigate to Settings>>>Certificate)
  Follow embedded help for instructions on how to configure it.

Deactivate unused features

Network module provides multiple options to upgrade firmware, change configurations, set power schedules, etc. The device also provide multiple options to connect with the device i.e. SSH, SNMP,SMTP,HTTPS etc. Services like SNMPv1 are considered insecure and Eaton recommends disabling all such insecure services.

- It is recommended to disable unused physical ports like USB and SD card.
- Disable insecure services like SNMP v1

Network Security

Network module provides network access to facilitate communication with other devices in the systems and configuration. But this capability could open up a big security hole if it's not configured securely.

Eaton recommends segmentation of networks into logical enclaves and restrict the communication to host-to-host paths. This helps protect sensitive information and critical services and limits damage from network perimeter breaches. At a minimum, a utility Industrial Control Systems network should be segmented into a three-tiered architecture (as recommended by NIST SP800-82[R3]) for better security control.

Deploy adequate network protection devices like Firewalls, Intrusion Detection / Protection devices,

Please find detailed information about various Network level protection strategies in Eaton Cybersecurity Considerations for Electrical Distribution Systems [R1]. Use the below information for configuring the firewalls to allow needed access for Network module to operate smoothly.

- Navigate to *Information>>>Specifications/Technical characteristics>>>Port* to get the list of all ports and services running on the device.
- SNMP V1/SNMP V3 can be disabled or configured by navigating to *Settings>>>SNMP*.
  Instructions are available in the *Contextual help>>>Settings>>>SNMP*.

Logging and Event Management

Best Practices

- Eaton recommends that all remote interactive sessions are encrypted, logged, and monitored including all administrative and maintenance activities.
- Ensure that logs are backed up, retain the backups for a minimum of 3 months or as per organization's security policy.
- Perform log review at a minimum every 15 days.
- Navigate to *Information>>>List of events codes* to get log information and how to export it.

Secure Maintenance

Best Practices

Apply Firmware updates and patches regularly

Due to increasing Cyber Attacks on Industrial Control Systems, Eaton implements a comprehensive patch and update process for its products. Users are encouraged to maintain a consistent process to promptly monitor for fresh firmware updates, implement patching and updates as and when required or released.

- Navigate in the help to *Contextual help>>>Card>>>Administration* to get information on how to upgrade the Network Module.
- Eaton also has a robust vulnerability response process. In the event of any security vulnerability getting discovered in its products, Eaton patches the vulnerability and releases information bulletin through its cybersecurity web site - http://eaton.com/cybersecurity and patch through www.powerquality.eaton.com/Support/.

Conduct regular Cybersecurity risk analyses of the organization /system.

Eaton has worked with third-party security firms to perform system audits, both as part of a specific customer's deployment and within Eaton's own development cycle process. Eaton can provide guidance and support to your organization's effort to perform regular cybersecurity audits or assessments.

Plan for Business Continuity / Cybersecurity Disaster Recovery

It's a Cybersecurity best practice for organizations to plan for Business continuity. Establish an OT Business Continuity plan, periodically review and, where possible, exercise the established continuity plans. Make sure offsite backups include

- Backup of the latest f/w copy of Network module. Make it a part of SOP to update the backup copy as soon as the latest f/w is updated on Network module.
- Backup of the most current configurations.
- Documentation of the most current User List.
- Save and store securely the current configurations of the device.

4.2.3 References

[R1] ***Cybersecurity Considerations for Electrical Distribution Systems (WP152002EN):***

http://www.eaton.com/ecm/groups/public/@pub/@eaton/@corp/documents/content/pct_1603172.pdf

[R2] ***Cybersecurity Best Practices Checklist Reminder (WP910003EN):***

http://www.cooperindustries.com/content/dam/public/powersystems/resources/library/1100_EAS/WP910003EN.pdf

[R3] ***NIST SP 800-82 Rev 2, Guide to Industrial Control Systems (ICS) Security, May 2015:***

https://ics-cert.us-cert.gov/Standards-and-References

[R4] National Institute of Technology (NIST) Interagency "Guidelines on Firewalls and Firewall Policy, NIST Special Publication 800-41", October 2009:

http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-41r1.pdf

4.3 Configuring user permissions through profiles

The user profile can be defined when creating a new users or changed when modifying an existing one.

Refer to the section Users in the settings.

4.4 Decommissioning the Network Management module

With the increased frequency of reported data breaches, it’s becoming more and more necessary for companies to implement effective and reliable decommissioning policies and procedures in order to protect the data stored on retired IT equipment from falling into the wrong hands, or a data breach.

Sanitization erases all the data (user name and password, certificates, keys, settings, logs...).

To sanitize the Network Module refer to: Sanitization

5 Servicing the EMP

5.1 Description and features

The optional Environmental Monitoring Probe (EMP) enables you to collect temperature and humidity readings and monitor the environmental data remotely.

You can also collect and retrieve the status of one or two dry contact devices (not included).

Up to 3 Environmental Monitoring Probe can be daisy chained on one device.

You can monitor readings remotely using SNMP or a standard Web browser through the Network module.

This provides greater power management control and flexible monitoring options.

The EMP device is delivered with a screw and screw anchor, magnets, nylon fasteners, tie wraps, and magnets. You can install the device anywhere on the rack or on the wall near the rack.

For more information, refer to the device manual.

The EMP has the following features:

- The hot-swap feature simplifies installation by enabling you to install the probe safely without turning off power to the device or to the loads that are connected to it.
- The EMP monitors temperature and humidity information to help you protect critical equipment.
- The EMP measures temperatures from 0°C to 70°C with an accuracy of ±2°C.
- The EMP measures relative humidity from 10% to 90% with an accuracy of ±5%.
- The EMP can be located some distance away from the device with a CAT5 network cable up to 50m (165 ft) long.
- The EMP monitors the status of the two user-provided contact devices.
- Temperature, humidity, and contact closure status can be displayed through a Web browser through the Network module or LCD interface (if available)
- A Temperature and Humidity Offset can be set.

5.2 Unpacking the EMP

The sensor will include the following:

- EMPDT1H1C2 sensor
- Dry contact terminal block
- Quickstart
- USB to RS485 converter
- RJ45 female to female connector
- Wall mounting screw and anchor
- Rack mounting screw nut and washer
- Tie wraps (x2)
- Nylon fastener

Packing materials must be disposed of in compliance with all local regulations concerning waste.
Recycling symbols are printed on the packing materials to facilitate sorting.

5.3 Installing the EMP

5.3.1 Defining EMPs address and termination

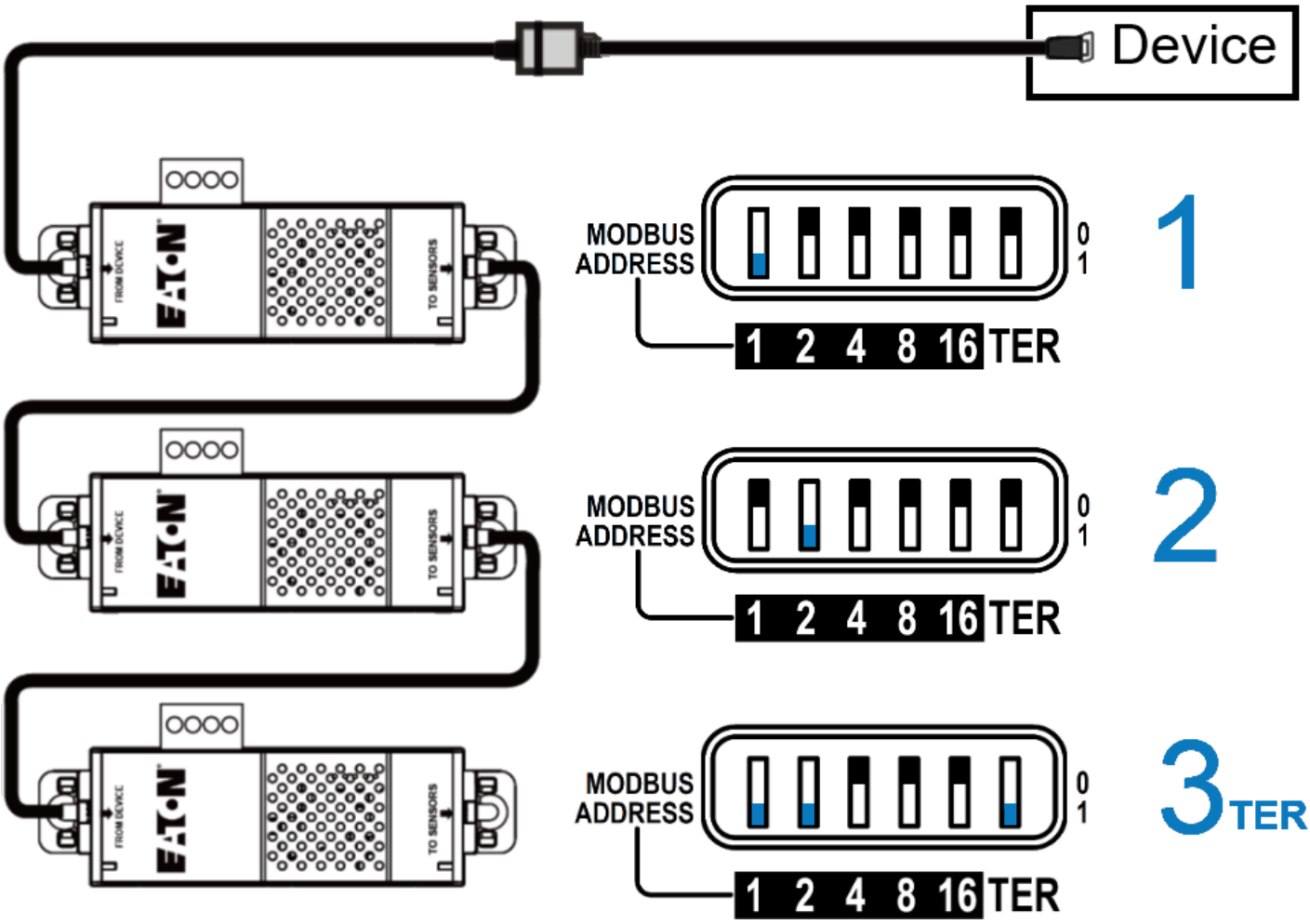
Manual addressing

> Address must be defined before the EMP power-up otherwise the changes won't be taken into account.
> Do not set Modbus address to 0, otherwise the EMP will not be detected.

Define **different address** for all the EMPs in the daisy-chain.

Set the RS485 termination (TER) to 1 on the last EMP of the daisy chain, set it to 0 on all the other EMPs.

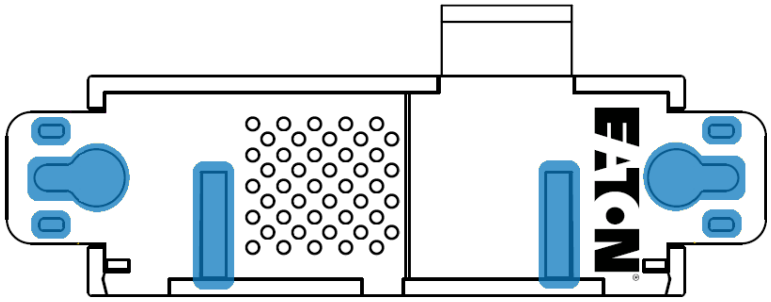
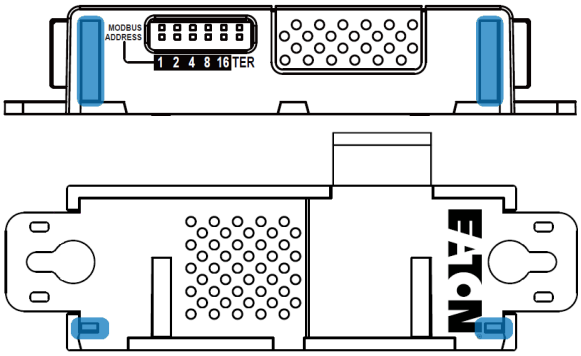
Example: manual addressing of 3 EMPs connected to the Device



> Green LED of the TO DEVICE RJ45 connector shows if the EMP is powered by the Network module.

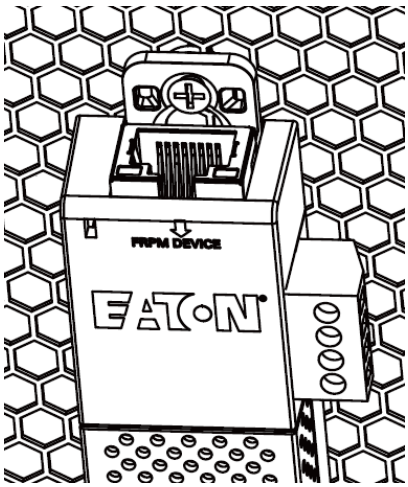
5.3.2 Mounting the EMP

The EMP includes magnets, cable ties slots and keyholes to enable multiple ways of mounting it on your installation.

Bottom mounting capabilities:	Side mounting
• magnets • keyholes • tie wraps • nylon fastener	• magnets • tie wraps
	

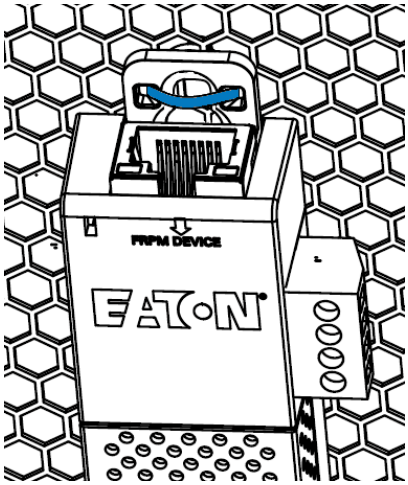
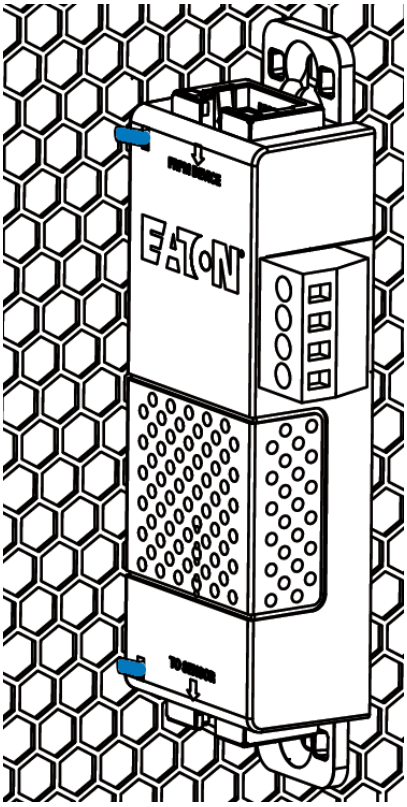
Rack mounting with keyhole example

To mount the EMP on the rack, use the supplied screw, washer and nut. Then, mount the EMP on the screw and tighten it.



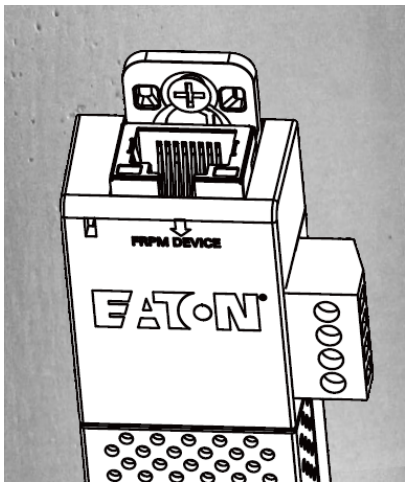
Rack mounting with tie wraps example

To mount the EMP on the door of the rack, use the supplied cable ties.

Bottom mounting	Side mounting
	

Wall mounting with screws example

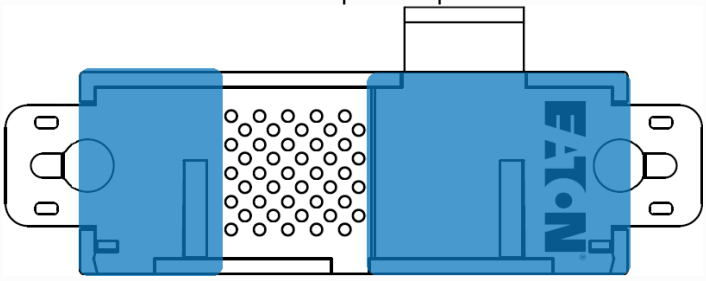
To mount the EMP on the wall close to the rack, use the supplied screw and screw anchor. Then, mount the EMP on the screw and tighten it.



Wall mounting with nylon fastener example

To mount the EMP within the enclosure environment, attach one nylon fastener to the EMP and the other nylon fastener to an enclosure rail post. Then, press the two nylon strips together to secure the EMP to the rail post.

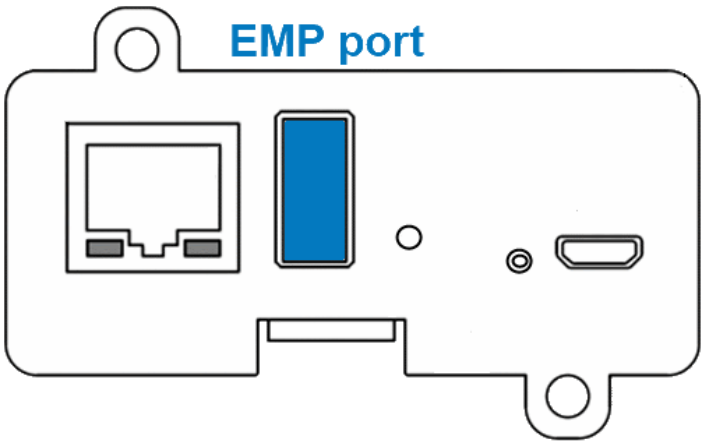
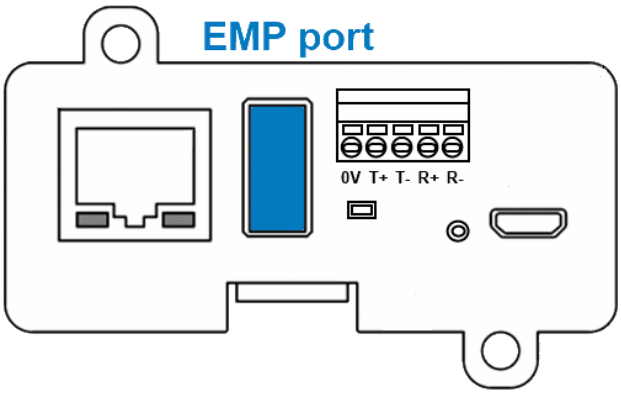
Cut nylon fastener and stick it on the EMP bottom on the location highlighted below, this will prevent to interfere with the EMP data acquisition parts.



5.3.3 Cabling the first EMP to the device

Available Devices

Network-M2 and INDGW-M2

Network-M2	INDGW-M2
	

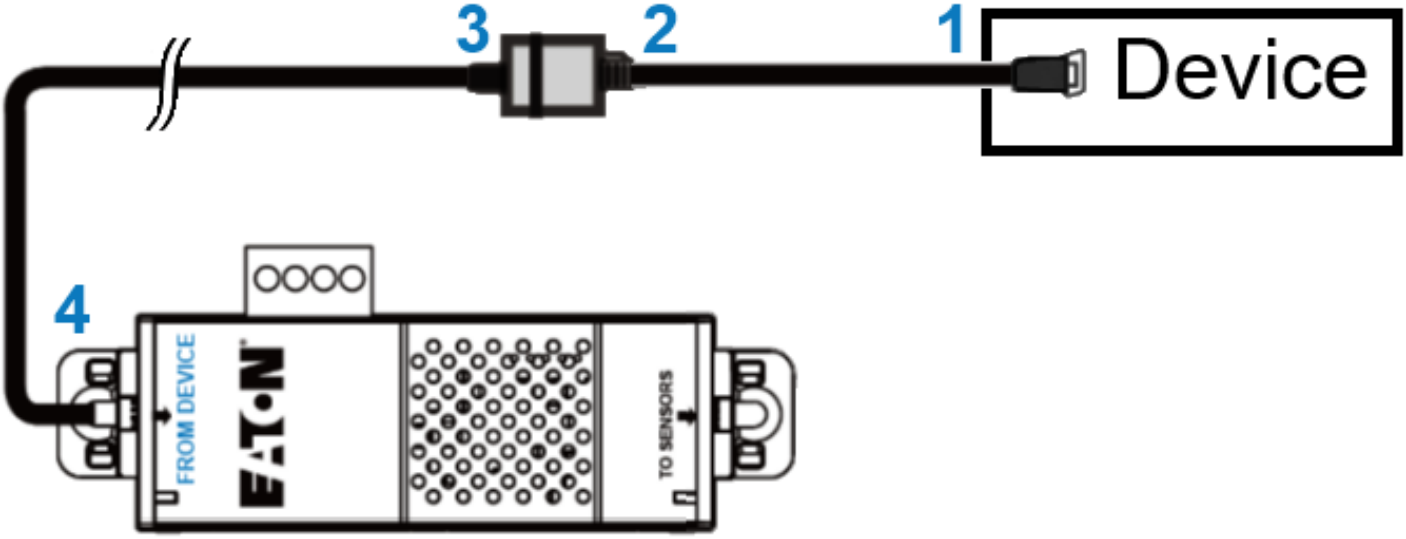
Connecting the EMP to the device

Address must be defined before the EMP power-up otherwise the changes won't be taken into account.
Do not set Modbus address to 0, otherwise the EMP will not be detected.

Material needed:

- EMP
- RJ45 female/female connector (supplied in EMP accessories)
- USB to RS485 converter cable (supplied in EMP accessories)
- Ethernet cable (**not supplied**).
- Device

Connection steps



Step 1 – Connect the "USB to RS485 converter cable" to the USB port of the Device.

Step 2 – Connect the "USB to RS485 converter cable" to the RJ45 female/female connector.

Step 3 – Connect the Ethernet cable to the other end of the RJ45 female/female connector.

Step 4 – Connect the other end of the Ethernet cable to the RJ-45 port on the EMP (FROM DEVICE).

Use the supplied tie wraps to secure the "RS485 to USB cable" to the Network cable.

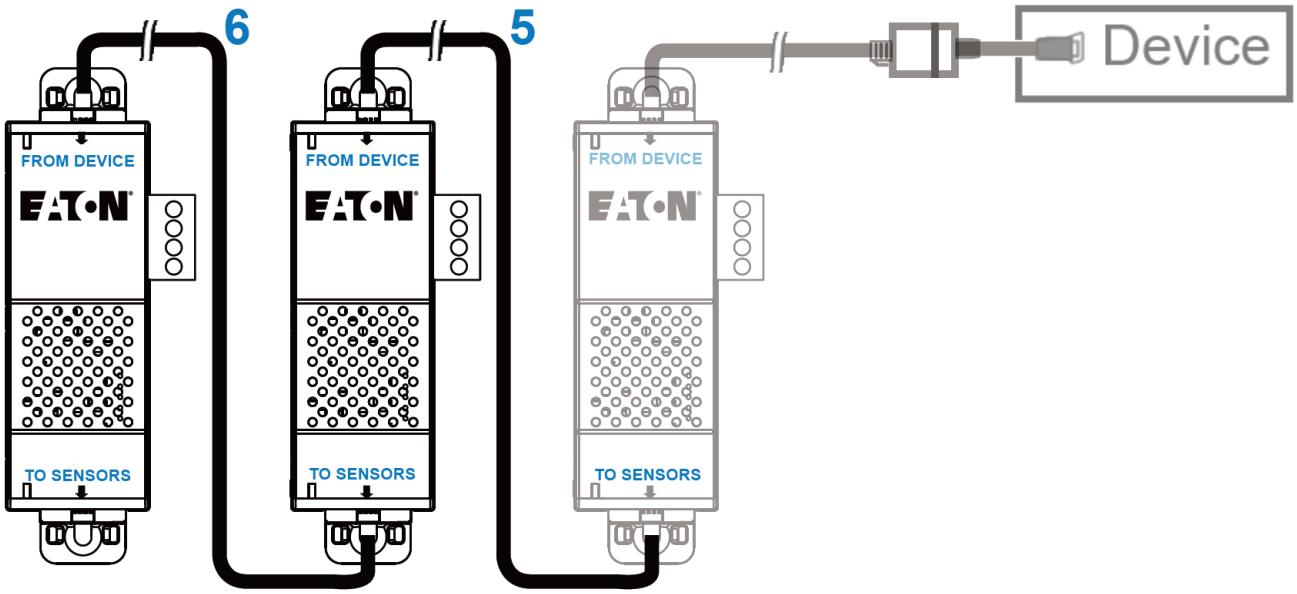
5.3.4 Daisy chaining EMPs

Address must be defined before the EMP power-up otherwise the changes won't be taken into account.
Do not set Modbus address to 0, otherwise the EMP will not be detected.

Material needed:

- First EMP connected to the device (refer to previous section)
- Additional EMPs
- 2 x Ethernet cable (**not supplied**).
- Device

Steps

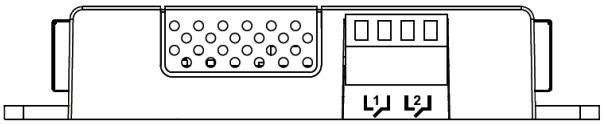


Up to 3 EMP can be daisy chained on one device.

STEP 5 – Connect the Ethernet cable to the "TO SENSORS" port of the first EMP, and to the "FROM DEVICE" port of the second EMP.

STEP 6 – Connect the Ethernet cable to the "TO SENSORS" port of the second EMP, and to the "FROM DEVICE" port of the third EMP.

5.3.5 Connecting an external contact device



To connect an external device to the EMP:

1- Connect the external contact closure inputs to the terminal block on the EMP (see the table and the figure below):

- External contact device 1. Connect the return and signal input wires from device 1 to screw terminals 1.
- External contact device 2. Connect the return and signal input wires from device 2 to screw terminals 2.

2- Tighten the corresponding tightening screws on top of the EMP to secure the wires.

5.4 Commissioning the EMP

5.4.1 On the Network-M2 device

STEP 1: Connect to the Network Module

- On a network computer, launch a supported web browser. The browser window appears.
- In the Address/Location field, enter: https://xxx.xxx.xxx.xxx/ where xxx.xxx.xxx.xxx is the IP address of the Network Module.
- The log in screen appears.
- Enter the user name in the User Name field.
- Enter the password in the Password field.
- Click **Sign In**. The Network Module web interface appears.

STEP 2: Navigate to **Cards/Commissioning** page

STEP 3: Proceed to the commissioning (refer to the contextual help for details: Cards>>>Commissioning (Sensors)

- Click **Discover**. The EMP connected to the Network module appears in the table.

When discovered, the orange LEDs of the EMP RJ45 connectors shows the data traffic.If the discovery process fails refer to the troubleshooting section.

The Sensor button on the left bar also appears, this will be reviewed on STEP4 .

- Press the pen logo to edit EMP information and access its settings.
- Click **Define offsets** to define temperature or humidity offsets if needed.

STEP 4: Define alarm configuration (refer to the contextual help for details: Sensors>>>Alarm configuration)

- Click on the **Sensors** menu that has just appeared on the left bar after the EMP discovery.
- Select the **Alarm configuration** page.
- Enable or disable alarms.
- Define thresholds, hysteresis and severity of temperature, humidity and dry contacts alarms.

5.5 Using the EMP for temperature compensated battery charging

This section applies only to UPS that provides temperature compensated battery charging option.

Address must be defined before the EMP is powered up; otherwise the changes won't be taken into account.
Do not set all the Modbus address to 0, otherwise the EMP will not be detected.
Define a **unique address** for all the EMPs in the daisy-chain.
Set the RS485 termination (TER) to 1 on the last EMP of the daisy chain. On other EMPs this should be set to 0.

5.5.1 Addressing the EMP

Set the address 31 to the sensor dedicated to the battery room temperature:

- Set all the Modbus address switches to 1 to set the EMP to the address 31 as indicated on the picture below:

5.5.2 Commissioning the EMP

Refer to the section Commissioning the EMP.

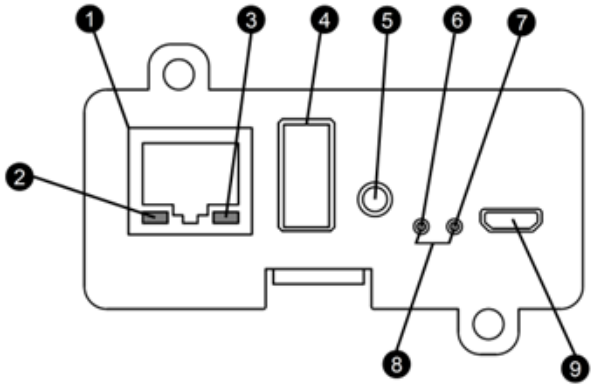
5.5.3 Enabling temperature compensated battery charging in the UPS

⚠ The temperature compensated battery charging feature needs to be enabled in the UPS.

To enable the temperature compensated battery charging, refer to the UPS user manual.

6 Information

6.1 Front panel connectors and LED indicators



Nbr	Name	Description
1	Network connector	Ethernet port
2	Network speed LED	Flashing green sequences: • 1 flash — Port operating at 10Mbps • 2 flashes — Port operating at 100Mbps • 3 flashes — Port operating at 1Gbps
3	Network link/activity LED	• Off — UPS Network Module is not connected to the network. • Solid yellow — UPS Network Module is connected to the network, but no activity detected. • Flashing yellow — UPS Network Module is connected to the network and sending or receiving data.
4	AUX connector	For Network Module accessories only. ⚠ ***Do not use for general power supply or USB charger.***
5	Restart button	Ball point pen or equivalent will be needed to restart: • Short press (<6s) — Safe software restart (firmware safely shutdown before restart). • Long press (>9s) — Forced hardware restart.
6	ON LED	Flashing green — Network Module is operating normally.
7	Warning LED	Solid red — Network Module is in error state.

❽	Boot LEDs	Solid green and flashing red — Network Module is starting boot sequence.
❾	Settings/UPS data connector	Configuration port. Access to Network Module's web interface through RNDIS (Emulated Network port). Access to the Network Module console through Serial (Emulated Serial port).

6.2 Default settings parameters

6.2.1 Settings

General

	Default setting	Possible parameters
General	Location — empty Contact — empty System name — empty	Location — 31 characters maximum Contact — 255 characters maximum System name — 255 characters maximum

Date & Time

	Default setting	Possible parameters
Date & Time	Mode — Manual (Time zone: Europe/ Paris)	Mode — Manual (Time zone: selection on map/ Date) / Dynamic (NTP)

Users

	Default setting	Possible parameters
Password strength	Minimum length — enabled (8) Minimum upper case — enabled (1) Minimum lower case — enabled (1) Minimum digit — enabled (1) Special character — enabled (1)	Minimum length — enable (6-32)/disable Minimum upper case — enable (0-32)/disable Minimum lower case — enable (0-32)/disable Minimum digit — enable (0-32)/disable Special character — enable (0-32)/disable
Account expiration	Password expires after — disabled Main administrator password never expires — disabled Block account when invalid password is entered after — disabled Main administrator account never blocks — disabled	Password expires after — disable/enable (1-99999) Main administrator password never expires — disable/enable Block account when invalid password is entered after — disable/enable (1-99) Main administrator account never blocks — disable/enable

Session expiration	No activity timeout — 60 minutes Session lease time — 120 minutes	No activity timeout — 1-60 minutes Session lease time — 60-720 minutes
Local users	1 user only: • Active — Yes • Profile — Administrator • Username — admin • Full Name — blank • Email — blank • Phone — blank • Organization — blank	10 users maximum: • Active — Yes/No • Profile — Administrator/Operator/Viewer • Username — 255 characters maximum • Full Name — 128 characters maximum • Email — 128 characters maximum • Phone — 64 characters maximum • Organization — 128 characters maximum

LDAP	Configure • Active – No • Security SSL – SSL Verify server certificate – enabled • Primary server Name – Primary Hostname – blank Port – 636 • Secondary server Name – blank Hostname – blank Port – blank • Credentials Anonymous search bind – disabled Search user DN – blank Password – blank • Search base Search base DN – dc=example,dc=com • Request parameters User base DN – ou=people,dc=example,dc=com User name attribute – uid UID attribute – uidNumber Group base DN – ou=group,dc=example,dc=com Group name attribute – gid GID attribute – gidNumber Profile mapping – no mapping Users preferences • Language –English • Temperature unit – °C (Celsius) • Date format – MM-DD-YYYY • Time format – hh:mm:ss (24h)	Configure • Active – No/yes • Security SSL – None/Start TLS/SSL Verify server certificate – disabled/enabled • Primary server Name – 128 characters maximum Hostname – 128 characters maximum Port – x-xxx • Secondary server Name – 128 characters maximum Hostname – 128 characters maximum Port – x-xxx • Credentials Anonymous search bind – disabled/enabled Search user DN – 1024 characters maximum Password – 128 characters maximum • Search base Search base DN – 1024 characters maximum • Request parameters User base DN – 1024 characters maximum User name attribute – 1024 characters maximum UID attribute – 1024 characters maximum Group base DN – 1024 characters maximum Group name attribute – 1024 characters maximum GID attribute – 1024 characters maximum Profile mapping – up to 5 remote groups mapped to local profiles Users preferences • Language –German/English/Spanish/French/ Italian/Japanese/Simplified Chinese/ Traditional Chinese • Temperature unit – °C (Celsius)/°F (Fahrenheit) • Date format – MM-DD-YYYY / YYY-MM-DD / DD-MM-YYY / DD.MM.YYY / DD/MM/YYY / DD MM YYYY • Time format – hh:mm:ss (24h) / hh:mm:ss (12h)

RADIUS	Configure • Active – No • Retry number – 0 • Primary server Name – blank Secret – blank Address – blank UDP port – 1812 Time out – 3 • Secondary server Name – blank Secret – blank Address – blank UDP port – 1812 Time out – 3 Users preferences • Language – English • Temperature unit – °C (Celsius) • Date format – MM-DD-YYYY • Time format – hh:mm:ss (24h)	Configure • Active – Yes/No • Retry number – 0 to 128 • Primary server Name – 128 characters maximum Address – 128 characters maximum Secret – 128 characters maximum UDP port – 1 to 65535 Time out – 3 to 60 • Secondary server Name – 128 characters maximum Address – 128 characters maximum Secret – 128 characters maximum UDP port – 1 to 65535 Time out – 3 to 60 Users preferences • Language – German/English/Spanish/French/Italian/ Japanese/Simplified Chinese/Traditional Chinese • Temperature unit – °C (Celsius) • Date format – MM-DD-YYYY • Time format – hh:mm:ss (24h)

Network

	Default setting	**Possible parameters**
LAN	Configuration — Auto negotiation	Configuration — Auto negotiation - 10Mbps - Half duplex - 10Mbps - Full duplex - 100Mbps - Half duplex - 100Mbps - Full duplex - 1.0 Gbps - Full duplex
IPV4	Mode — Dynamic (DHCP)	Mode — DHCP/Manual (IP address/Netmask/Gateway)
Domain	Domain configuration (more) : • Hostname — ups-[MAC address] • Mode — DHCP	Domain configuration (more) : • Hostname — 128 characters maximum • Mode :DHCP/Manual (Domain name/Primary DNS/ Secondary DNS)
IPV6	Enable — checked IPV6 details (more) : • Mode — Router	Enable — enable/disable IPV6 details (more) : • Mode — Router/Manual (Address/Prefix/Gateway)

Protocols

	Default setting	**Possible parameters**
HTTPS	Port — 443	Port — x-xxx

Syslog	Enable — disabled • Server#1 Name – Primary Active – No Hostname – empty Port – 514 Protocol – UDP Message transfer method – Non transparent framing Using unicode byte order mask (BOM) – disabled • Server#2 Name – empty Active – No Hostname – empty Port – 514 Protocol – UDP Message transfer method – DIsabled in UDP Using unicode byte order mask (BOM) – disabled	Enable — disable/enable • Server#1 Name – 128 characters maximum Active – No/Yes Hostname – 128 characters maximum Port – x-xxx Protocol – UDP/TCP Message transfer method – Non transparent framing Using unicode byte order mask (BOM) – disable/enable • Server#2 Name – 128 characters maximum Active – No/Yes Hostname – 128 characters maximum Port – x-xxx Protocol – UDP/TCP Message transfer method (in TCP) – Octet counting/Non transparent framing Using unicode byte order mask (BOM) – disable/enable

SNMP

	Default setting	Possible parameters
SNMP	Enable — disabled Port — 161 SNMP V1 — disabled • Community #1 — public Active — No Access — Read only • Community #2 — private Active — No Access — Read/Write SNMP V3 — enabled • User #1 — readonly Active — No Access — Read only Authentication — Auth (SHA-1) Password — empty Confirm password — empty Privacy — Secured - AES Key — empty Confirm key — empty • User#2 — readwrite Active — No Access — Read/Write Authentication — Auth (SHA-1) Password — empty Confirm password — empty Privacy — Secured - AES Key — empty Confirm key — empty	Enable — disable/enable Port — x-xxx SNMP V1 — disable/enable • Community #1 — 128 characters maximum Active — No/Yes Access — Read only • Community #2 — 128 characters maximum Active — No/Yes Access — Read/Write SNMP V3 — disable/enable • User #1 — 32 characters maximum Active — No/Yes Access — Read only/Read-Write Authentication — Auth (SHA-1)/None Password — 128 characters maximum Confirm password — 128 characters maximum Privacy — Secured - AES/None Key — 128 characters maximum Confirm key — 128 characters maximum • User#2 — 32 characters maximum Active — No/Yes Access — Read only/Read-Write Authentication — Auth (SHA-1)/None Password — 128 characters maximum Confirm password — 128 characters maximum Privacy — Secured - AES/None Key — 128 characters maximum Confirm key — 128 characters maximum
Trap receivers	No trap	Active — No/Yes Application name — 128 characters maximum Hostname or IP address — 128 characters maximum Port — x-xxx Protocol — V1 Trap community — 128 characters maximum

Email

	Default setting	Possible parameters
Email sending configuration	No email	5 configurations maximum Active — No/Yes Configuration name — 128 characters maximum Email address — 128 characters maximum • Notify on events Active — No/Yes On card events – Subscribe/Attach logs (Critical/Warning/Info) On devices events – Subscribe/Attach logs (Critical/Warning/Info) Exceptions on events notification – Always notify events with code/Never notify events with code • Periodic report Active — No/Yes Recurrence – Every day/Every week/Every month Starting – Date and time Topic – Subscribe/Attach logs (Card/Devices) • Email configuration Sender – text field/list of customization key words Subject – text field/list of customization key words
SMTP	Server IP/Hostname — blank SMTP server authentication — disabled Port — 25 Sender address — ups@networkcard.com Secure SMTP connection — enabled Verify certificate authority — disabled	Server IP/Hostname — 128 characters maximum SMTP server authentication — disable/enable (Username/Password — 128 characters maximum) Port — x-xxx Sender address — 128 characters maximum Secure SMTP connection — enable/disable Verify certificate authority — disable/enable

My preferences

	Default setting	Possible parameters
Profile	Edit user: • Full name — Administrator • Email — blank • Phone — blank • Organization — blank	Edit user: • Full name — 128 characters maximum • Email — 128 characters maximum • Phone — 64 characters maximum • Organization — 128 characters maximum
Temperature	°C (Celsius)	°C (Celsius)/°F (Fahrenheit)

Date format	MM-DD-YYYY	MM-DD-YYYY / YYY-MM-DD / DD-MM-YYY / DD.MM.YYY / DD/ MM/YYY / DD MM YYYY
Time format	hh:mm:ss (24h)	hh:mm:ss (24h) / hh:mm:ss (12h)
Language	English	Language —German/English/Spanish/French/Italian/ Japanese/Simplified Chinese/Traditional Chinese

6.2.2 Meters

	Default setting	**Possible parameters**
Configuration	Log measures every — 60s	Log measures every — 3600s maximum

6.2.3 Sensors alarm configuration

	Default setting	**Possible parameters**
Temperature	Enabled — No Low critical – 0°C/32°F Low warning – 10°C/50°F High warning – 70°C/158°F High critical – 80°C/176°F	Enabled — No/Yes low critical<low warning<high warning<high critical
Humidity	Enabled — No Low critical – 10% Low warning – 20% High warning – 80% High critical – 90%	Enabled — No/Yes 0%<low critical<low warning<high warning<high critical<100%
Dry contacts	Enabled — No Alarm severity – Warning	Enabled — No/Yes Alarm severity – Info/Warning/Critical

6.3 Specifications/Technical characteristics

Physical characteristics	
Dimensions (wxdxh)	132 x 66 x 42 mm | 5.2 x 2.6 x 1.65 in
Weight	70 g | 0.15 lb
RoHS	100% compatible
Storage	
Storage temperature	-25°C to 70°C (14°F to 158°F)
Ambient conditions	
Operating temperature	0°C to 70°C (32°F to 158°F)
Relative humidity	5%-95%, noncondensing
Module performance	
Module input power	5V-12V ±5% | 1A
AUX output power	5V ±5% | 200mA
Date/Time backup	CR1220 battery coin cell | The RTC is able to keep the date and the time when Network Module is OFF
Functions	
Languages	English, French, Italian, German, Spanish, Japanese,
Alarms/Log	Email, SNMP trap, web interface / Log on events
Network	Gigabit ETHERNET, 10/100/1000Mb/s, auto negotiation, HTTP 1.1, SNMP V1, SNMP V3, NTP, SMTP, DHCP
Security	Restricted to TLS 1.2
Supported MIBs	*xUPS MIB* | *Standard IETF UPS MIB (RFC 1628)* | *Sensor MIB*
Browsers	Internet Explorer, Google Chrome, Firefox, Safari
Settings (default values)	
IP network	DHCP enabled | NTP server: pool.ntp.org
Port	443 (https), 22 (ssh), 161 (snmp), 162 (snmp trap), 25 (smtp), 8883 (mqtts), 123 (ntp), 5353 (mdns-sd), 80 (http), 514 (syslog),636 (LDAP), 1812 (RADIUS)

Web interface access control	User name: admin | Password: admin
Settings/UPS data connector	USB RNDIS Apipa compatible | IP address: 169.254.0.1 | Subnet mask: 255.255.0.0

6.4 List of event codes

To get access to the Alarm log codes or the System log codes for email subscription, see the Alarm log codes and System log codes sections.

6.5 Alarm log codes

To retrieve Alarm logs, navigate to Alarm section and press the **Download alarms** button.

6.5.1 Critical

Code	Severity	Active message	Non-active message	Advice
002	Critical	Internal failure	End of internal failure	Service required
004	Critical	Temperature alarm	Temperature OK	Check air conditioner
007	Critical	Fan fault	Fan OK	Service required
00F	Critical	Parallel UPS not compatible	Parallel UPS compatibility OK	Service required
010	Critical	UPS power supply fault	UPS power supply OK	Service required
011	Critical	Parallel UPS protection lost	Parallel UPS protection OK	Reduce output load
012	Critical	Parallel UPS measure inconsistent	Parallel UPS measure OK	Service required
100	Critical	Rectifier fuse fault	Rectifier fuse OK	Service required
105	Critical	Input AC module failure	Input AC module OK	Service required
110	Critical	Building alarm (through dry contact)	Building alarm OK	-
11F	Critical	Building alarm (through Network module)	Building alarm OK	-
202	Critical	Bypass thermal overload	Bypass thermal OK	Reduce output load
203	Critical	Bypass temperature alarm	Bypass temperature OK	Check air conditioner
207	Critical	Bypass AC module failure	Bypass AC module OK	-
208	Critical	Bypass overload	No bypass overload	-
305	Critical	Rectifier failure	Rectifier OK	Service required

306	Critical	Rectifier overload	Rectifier OK	Reduce output load
308	Critical	Rectifier short circuit	Rectifier OK	Reduce output load
400	Critical	DCDC converter failure	DCDC converter OK	Service required
500	Critical	Battery charger fault	Battery charger OK	Service required
600	Critical	Battery fuse fault	Battery fuse OK	Service required
602	Critical	Battery fuse fault	Battery fuse OK	Service required
604	Critical	Battery low	Battery OK	-
607	Critical	Battery test failed	Battery test OK	Check battery
60D	Critical	No battery	Battery present	Check battery
629	Critical	Battery voltage low critical	Battery voltage OK	Check battery
62B	Critical	Battery voltage high critical	Battery voltage OK	Check battery
62D	Critical	Battery charge current low critical	Battery charge current OK	Check battery
62F	Critical	Battery charge current high critical	Battery charge current OK	Check battery
631	Critical	Battery discharge current low critical	Battery discharge current OK	Check battery
633	Critical	Battery discharge current high critical	Battery discharge current OK	Check battery
635	Critical	Battery temperature low critical	Battery temperature OK	Check battery
637	Critical	Battery temperature high critical	Battery temperature OK	Check battery
63E	Critical	Battery fault	Battery OK	Check battery
700	Critical	Inverter limitation	No current limitation	Reduce output load
701	Critical	Inverter fuse fault	Inverter fuse OK	Service required
704	Critical	Inverter internal failure	UPS OK	Service required
705	Critical	Inverter overload	No power overload	Reduce output load
706	Critical	Temperature alarm	Temperature OK	Check air conditioner
70A	Critical	Inverter thermal overload	No power overload	Reduce output load
70B	Critical	Inverter short circuit	End of inverter short circuit	Service required

802	Critical	Shutdown imminent	Shutdown canceled	-
805	Critical	Output short circuit	Output OK	Reduce output load
806	Critical	Emergency power OFF	No emergency OFF	-
811	Critical	Parallel negative power	Parallel power OK	Reduce output load
814	Critical	Firmware watchdog reset	Firmware watchdog OK	Service required
815	Critical	Calibration fault	Calibration OK	Service required
81E	Critical	Load unprotected	Load protected	-
900	Critical	Maintenance bypass	Not on maintenance bypass	-
1201	Critical	Temperature is critically low *(EMP)*	Temperature is back to low *(EMP)*	-
1204	Critical	Temperature is critically high *(EMP)*	Temperature is back to high *(EMP)*	-
1211	Critical	Humidity is critically low *(EMP)*	Humidity is back to low *(EMP)*	-
1214	Critical	Humidity is critically high *(EMP)*	Humidity is back to high *(EMP)*	-

6.5.2 Warning

Code	Severity	Active message	Non-active message	Advice
001	Warning	On battery	No more on battery	-
00B	Warning	Parallel UPS redundancy lost	Parallel UPS redundancy OK	Reduce output load
00E	Warning	Parallel UPS communication lost	Parallel UPS communication OK	Service required
103	Warning	Utility breaker open	Utility breaker closed	-
104	Warning	Input AC frequency out of range	Input AC frequency in range	-
106	Warning	Input AC not present	Input AC present	-
107	Warning	Input bad wiring	Input wiring OK	Check input wiring
108	Warning	Input AC voltage out of range (-)	Input AC voltage in range	-

109	Warning	Input AC voltage out of range (+)	Input AC voltage in range	-
10A	Warning	Input AC unbalanced	End of input AC unbalanced	-
200	Warning	Bypass phase out range	Bypass phase in range	-
201	Warning	Bypass not available	Bypass available	Service required
204	Warning	Bypass breaker open	Bypass breaker closed	-
205	Warning	Bypass mode	No more on bypass	-
206	Warning	Bypass frequency out of range	Bypass frequency in range	-
209	Warning	Bypass voltage out of range	Bypass voltage in range	-
20A	Warning	Bypass AC over voltage	End of bypass AC over voltage	-
20B	Warning	Bypass AC under voltage	End of bypass AC under voltage	-
20C	Warning	Bypass bad wiring	Bypass wiring OK	Check bypass wiring
300	Warning	DC bus + too high	DC bus + voltage OK	Service required
301	Warning	DC bus - too high	DC bus - voltage OK	Service required
302	Warning	DC bus + too low	DC bus + voltage OK	Service required
303	Warning	DC bus - too low	DC bus - voltage OK	Service required
304	Warning	DC bus unbalanced	DC bus OK	Service required
501	Warning	Charger temperature alarm	Charger temperature OK	Service required
502	Warning	Max charger voltage	Charger voltage OK	Service required
503	Warning	Min charger voltage	Charger voltage OK	Service required
603	Warning	Battery discharging	End of UPS battery discharge	-
605	Warning	Battery temperature alarm	Battery temperature OK	Service required
606	Warning	Battery breaker open	Battery breaker closed	Service required
610	Warning	Battery low voltage	Battery voltage OK	Check battery
613	Warning	Battery voltage too high	Battery voltage OK	Check battery
616	Warning	Battery voltage unbalanced	Battery voltage OK	Check battery
61C	Warning	Communication with battery lost	Communication with battery recovered	Check battery

61E	Warning	At least one breaker in battery is open	All battery breakers are closed	Check battery
61F	Warning	Battery State Of Charge below limit	Battery State Of Charge OK	-
620	Warning	Battery State Of Health below limit	BatteryState Of Health OK	Check battery
628	Warning	Battery voltage low warning	Battery voltage OK	Check battery
62A	Warning	Battery voltage high warning	Battery voltage OK	Check battery
62C	Warning	Battery charge current low warning	Battery charge current OK	Check battery
62E	Warning	Battery charge current high warning	Battery charge current OK	Check battery
630	Warning	Battery discharge current low warning	Battery discharge current OK	Check battery
632	Warning	Battery discharge current high warning	Battery discharge current OK	Check battery
634	Warning	Battery temperature low warning	Battery temperature OK	Check battery
636	Warning	Battery temperature high warning	Battery temperature OK	Check battery
638	Warning	Battery BMS failure	Battery BMS OK	Check battery
639	Warning	Battery temperature unbalanced	Battery temperature OK	Check battery
63D	Warning	Battery warning	Battery OK	Check battery
70C	Warning	Inverter voltage too low	Inverter voltage OK	Service required
70D	Warning	Inverter voltage too high	Inverter voltage OK	Service required
801	Warning	Load not powered	Load powered	-
803	Warning	Output breaker open	Output breaker closed	-
808	Warning	Power overload	No power overload	Reduce output load
80D	Warning	Internal configuration failure	Internal configuration OK	Service required
80E	Warning	Overload pre-alarm	No overload pre-alarm	Reduce output load
810	Warning	Overload alarm	No overload	Reduce output load
816	Warning	Compatibility failure	Compatibility OK	Service required

817	Warning	Output over current	No output over current	Reduce output load
818	Warning	Output frequency out of range	Output frequency in range	Service required
819	Warning	Output voltage too high	Output voltage OK	Service required
81A	Warning	Output voltage too low	Output voltage OK	Service required
81B	Warning	UPS Shutoff requested	End of UPS shutoff requested	Service required
81D	Warning	Load not powered	Load protected	-
901	Warning	Maintenance bypass breaker closed	Maintenance bypass breaker open	-
B00	Warning	End of warranty	End of warranty cleared	-
B01	Warning	Batteries are aging. Consider replacement	Batteries aging condition cleared	-
1032	Warning	Protection: immediate shutdown in progress	Protection: immediate shutdown completed	-
1053	Warning	Protection: communication lost with agent	Protection: communication recovered with agent	-
1200	Warning	Communication lost *(with EMP)*	Communication recovered *(EMP)*	-
1202	Warning	Temperature is low *(EMP)*	Temperature is back to normal *(EMP)*	-
1203	Warning	Temperature is high *(EMP)*	Temperature is back to normal *(EMP)*	-
1212	Warning	Humidity is low *(EMP)*	Humidity is back to normal *(EMP)*	-
1213	Warning	Humidity is high *(EMP)*	Humidity is back to normal *(EMP)*	-

6.5.3 Info

Code	Severity	Active message	Non-active message	Advice
005	Info	Communication lost (with UPS)	Communication recovered (with UPS)	Service required
009	Info	On high efficiency	High efficiency disabled	-
013	Info	Upgrading: limited communication	End of upgrade mode	-

101	Info	On AVR (Boost)	End of AVR (Boost)	-
102	Info	On AVR (Buck)	End of AVR (Buck)	-
63C	Info	Battery information	Battery OK	-
A00	Info	Group 1 is OFF	Group 1 is ON	-
A01	Info	Group 2 is OFF	Group 2 is ON	-
A0F	Info	Group is OFF	Group is ON	-
1016	Info	Protection: sequential shutdown scheduled	Protection: sequential shutdown canceled	-
1017	Info	Protection: sequential shutdown in progress	Protection: sequential shutdown completed	-
1054	Info	Protection: agent is in unknown state	Protection: agent is in service	-
1055	Info	Protection: agent is starting	Protection: agent is in service	-
1056	Info	Protection: agent is stopping	Protection: agent is in service	-
1057	Info	Protection: agent is stopped	Protection: agent is in service	-
1100	Info	Schedule: shutdown date reached	Schedule: shutdown initiated	-
1101	Info	Schedule: restart date reached	Schedule: restart initiated	-
1300	Info	No UPS connected	Communication recovered (with UPS)	-
1301	Info	UPS not supported	Communication recovered (with UPS)	-

6.5.4 With settable severity

Code	Severity	Active message	Non-active message	Advice
1221	Settable	Contact is active *(EMP)*	Contact is back to normal *(EMP)*	-

6.6 System log codes

To retrieve System logs, navigate to Card>>>System logs section and press the **Download System logs** button.

6.6.1 Critical

Code	Severity	Log message	File
0801000	Alert	User account - admin password reset to default	logAccount.csv
0E00400	Critical	The [selfsign/PKI] signed certificate of the <service> server is not valid	logSystem.csv
0A00700	Error	Network module file system integrity corrupted <f/w: xx.yy.zzzz>	logUpdate.csv
0000D00	Error	Card reboot due to database error	logSystem.csv

6.6.2 Warning

Code	Severity	Log message	File
0A00200	Warning	Network module upgrade failed <f/w: xx.yy.zzzz>	logUpdate.csv
0A00A00	Warning	Network module bootloader upgrade failed <f/w: xx.yy.zzzz>	logUpdate.csv
0B00500	Warning	RTC battery cell low	logSystem.csv
0E00200	Warning	New [self/PKI] signed certificate [generated/imported] for <service> server	logSystem.csv
0E00300	Warning	The [self/PKI] signed certificate of the <service> server will expires in <X> days	logSystem.csv
0800700	Warning	User account - password expired	logAccount.csv
0800900	Warning	User account- locked	logAccount.csv
0F01300	Warning	Card reboot due to UPS FW upgrade	logSystem.csv
1000F00	Warning	<*feature*> settings partial restoration	logSystem.csv
1001000	Warning	<*feature*> settings restoration error	logSystem.csv
1000C00	Warning	Settings partial restoration	logSystem.csv
1000D00	Warning	Settings restoration error	logSystem.csv

6.6.3 Info

Code	Severity	Log message	File
0300D00	Notice	User action - sanitization launched	logSystem.csv
0A00500	Notice	Network module sanitized	logUpdate.csv
0A00900	Notice	Network module bootloader upgrade success <f/w: xx.yy.zzzz>	logUpdate.csv
0A00B00	Notice	Network module bootloader upgrade started <f/w: xx.yy.zzzz>	logUpdate.csv
0A00C00	Notice	Periodic system integrity check started	logUpdate.csv
0B00100	Notice	Time manually changed	logSystem.csv
0B00700	Notice	NTP sever not available <NTP server address>	logSystem.csv
0900100	Notice	Session - opened	logSession.csv
0900200	Notice	Session - closed	logSession.csv
0900300	Notice	Session - invalid token	logSession.csv
0900400	Notice	Session - authentication failed	logSession.csv
0300F00	Notice	User action - network module admin password reset switch activated	logSystem.csv
0E00500	Notice	[Certificate authority/ Client certificate] <id> is added for <service>	logSystem.csv
0E00600	Notice	[Certificate authority/ Client certificate] <id> is revoked for <service>	logSystem.csv
0800100	Notice	User account - created <user account id>	logAccount.csv
0800200	Notice	User account - deleted <user account id>	logAccount.csv
0800400	Notice	User account - name changed <user account id>	logAccount.csv
0800600	Notice	User account - password changed	logAccount.csv
0800800	Notice	User account- password reset <user account id>	logAccount.csv
0800A00	Notice	User account- unlocked	logAccount.csv
0800B00	Notice	User account - activated <user account id>	logAccount.csv
0800C00	Notice	User account - deactivated <user account id>	logAccount.csv
0800D00	Notice	User account - password rules changed	logAccount.csv
0800E00	Notice	User account - password expiration changed	logAccount.csv

0800F00	Notice	User account - session expiration changed	logAccount.csv
0900D00	Notice	<user> connected into interactive CLI with session id XXXXXX	logSession.csv
0900E00	Notice	<user> disconnected from interactive CLI with session id XXXXXX	logSession.csv
0900F00	Notice	<user> doesn't have access to CLI - CLI session id XXXXXX	logSession.csv
0901000	Notice	<user> connected and executes remote command <command> into the CLI - CLI session id XXXXXX	logSession.csv
0901100	Notice	<user> finished executing remote command <command> into the CLI - CLI session id XXXXXX	logSession.csv
0901200	Notice	<user> connection rejected - CLI session id XXXXXX	logSession.csv
0901300	Notice	<user> disconnected from interactive CLI with session id XXXXXX due to session timeout	logSession.csv
0901400	Notice	<user> disconnected from interactive CLI with session id XXXXXX due to concurrent connection with session id XXXXXX	logSession.csv
0100C00	Notice	Syslog is started	logSystem.csv
0100B00	Notice	Syslog is stopping	logSystem.csv
0100D00	Notice	Network module is booting	logSystem.csv
0100E00	Notice	Network module is operating	logSystem.csv
0100F00	Notice	Network module is starting shutdown sequence	logSystem.csv
0101000	Notice	Network module is ending shutdown sequence	logSystem.csv
0101400	Notice	Network module shutdown requested	logSystem.csv
0101500	Notice	Network module reboot requested	logSystem.csv
0A00100	Info	Network module upgrade success <f/w: xx.yy.zzzz>	logUpdate.csv
0A00300	Info	Network module upgrade started	logUpdate.csv
0A00600	Info	Network module file system integrity OK <f/w: xx.yy.zzzz>	logUpdate.csv
0B00300	Info	Time with NTP synchronized	logSystem.csv
0B00600	Info	Time settings changed	logSystem.csv
0B01100	Info	Time reset to last known date: "date"	logSystem.csv
1000100	Info	Settings saving requested	logSystem.csv
1000200	Info	<*feature*> settings saved	logSystem.csv
1000A00	Info	Settings restoration requested	logSystem.csv

1000E00	Info	<*feature*> settings restoration success	logSystem.csv
1000B00	Info	Settings restoration success	logSystem.csv
0301500	Notice	Sanitization switch changed	logSystem.csv
0A01600	Notice	Major version downgrade	logUpdate.csv

6.7 SNMP traps

6.7.1 Sensor Mib traps

This information is for reference only.

Trap oid : .1.3.6.1.4.1.534.6.8.1.x.x.x	**Trap description**
.1.3.6.1.4.1.534.6.8.1.**1.0.1**	Sent whenever the sensor count changes after a discovery or removing from the UI.
.1.3.6.1.4.1.534.6.8.1.**1.0.2**	Sent whenever one status of each sensor connected changes.
.1.3.6.1.4.1.534.6.8.1.**2.0.1**	Sent whenever one status of each temperature changes.
.1.3.6.1.4.1.534.6.8.1.**3.0.1**	Sent whenever one status of each humidity changes.
.1.3.6.1.4.1.534.6.8.1.**4.0.1**	Sent whenever one status of each digital input alarm changes.

6.7.2 Xups Mib traps

This information is for reference only.

Trap oid : .1.3.6.1.4.1.534.1.11.4.1.0.x	**Trap message at oid : .1.3.6.1.4.1.534.1.11.3.0**
.1.3.6.1.4.1.534.1.11.4.1.0.3	Battery discharging
.1.3.6.1.4.1.534.1.11.4.1.0.4	Battery low
.1.3.6.1.4.1.534.1.11.4.1.0.5	No more on battery
.1.3.6.1.4.1.534.1.11.4.1.0.6	Battery OK
.1.3.6.1.4.1.534.1.11.4.1.0.7	Power overload
.1.3.6.1.4.1.534.1.11.4.1.0.8	Internal failure
.1.3.6.1.4.1.534.1.11.4.1.0.10	Inverter internal failure
.1.3.6.1.4.1.534.1.11.4.1.0.11	Bypass mode
.1.3.6.1.4.1.534.1.11.4.1.0.12	Bypass not available
.1.3.6.1.4.1.534.1.11.4.1.0.13	Load not powered
.1.3.6.1.4.1.534.1.11.4.1.0.14	On battery
.1.3.6.1.4.1.534.1.11.4.1.0.15	Building alarm through input dry contact
.1.3.6.1.4.1.534.1.11.4.1.0.16	Shutdown imminent

Trap oid : .1.3.6.1.4.1.534.1.11.4.1.0.x	Trap message at oid : .1.3.6.1.4.1.534.1.11.3.0
.1.3.6.1.4.1.534.1.11.4.1.0.17	No more on bypass
.1.3.6.1.4.1.534.1.11.4.1.0.20	Breaker open
.1.3.6.1.4.1.534.1.11.4.1.0.23	Battery test failed
.1.3.6.1.4.1.534.1.11.4.1.0.26	Communication lost
.1.3.6.1.4.1.534.1.11.4.1.0.30	Sensor contact is active
.1.3.6.1.4.1.534.1.11.4.1.0.31	Sensor contact back to normal
.1.3.6.1.4.1.534.1.11.4.1.0.32	Parallel UPS redundancy lost
.1.3.6.1.4.1.534.1.11.4.1.0.33	Temperature alarm
.1.3.6.1.4.1.534.1.11.4.1.0.34	Battery charger fault
.1.3.6.1.4.1.534.1.11.4.1.0.35	Fan fault
.1.3.6.1.4.1.534.1.11.4.1.0.36	Fuse fault
.1.3.6.1.4.1.534.1.11.4.1.0.42	Sensor temperature is below/above critical threshold
.1.3.6.1.4.1.534.1.11.4.1.0.43	Sensor humidity is below/above critical threshold
.1.3.6.1.4.1.534.1.11.4.1.0.48	Maintenance bypass

6.7.3 IETF Mib-2 Ups traps

This information is for reference only.

Trap oid : .1.3.6.1.2.1.33.2.0.x	Description :	
.1.3.6.1.2.1.33.2.0.**1**	Sent whenever the UPS transfers on battery, then sent every minutes until the UPS Comes back to AC Input.	
.1.3.6.1.2.1.33.2.0.**3**	Sent whenever an alarm appears. The matching alarm oid is added as binded variables in the table below.	
.1.3.6.1.2.1.33.2.0.4	Sent whenever an alarm disappears. The matching alarm oid is added as binded variables in the table below.	
Alarm oid at : .1.3.6.1.2.1.33.1.6.3.x	**Description when trap 3**	**Description when trap 4**
.1.3.6.1.2.1.33.1.6.3.**1**	Battery test failed	Battery test OK
.1.3.6.1.2.1.33.1.6.3.**2**	Battery discharging	End of UPS battery discharge

Alarm oid at : .1.3.6.1.2.1.33.1.6.3.x	Description when trap 3	Description when trap 4
.1.3.6.1.2.1.33.1.6.3.**3**	Low battery	Battery OK
.1.3.6.1.2.1.33.1.6.3.**5**	Temperature alarm	Temperature OK
.1.3.6.1.2.1.33.1.6.3.**6**	Input AC not present	Input AC present
.1.3.6.1.2.1.33.1.6.3.**8**	Power overload	No power overload
.1.3.6.1.2.1.33.1.6.3.**9**	Bypass mode	No more on bypass
.1.3.6.1.2.1.33.1.6.3.**10**	Bypass not available	Bypass available
.1.3.6.1.2.1.33.1.6.3.**13**	Battery charger fault	Battery charger OK
.1.3.6.1.2.1.33.1.6.3.**14**	Not powered	Powered (Protected or Not protected)
.1.3.6.1.2.1.33.1.6.3.**16**	Fan fault	Fan OK
.1.3.6.1.2.1.33.1.6.3.**17**	Battery fuse fault Rectifier fuse fault Inverter fuse fault	Battery fuse OK Rectifier fuse OK Inverter fuse OK
.1.3.6.1.2.1.33.1.6.3.**18**	Internal failure	End of internal failure
.1.3.6.1.2.1.33.1.6.3.**20**	Communication lost	Communication recovered
.1.3.6.1.2.1.33.1.6.3.**23**	Shutdown imminent	Shutdown canceled

6.8 CLI

CLI can be accessed through:

- SSH
- Serial terminal emulation (refer to section Servicing the Network Management Module>>>Installing the Network Module>>>Accessing the card through serial terminal emulation).

It is intended mainly for automated configuration of the network and time settings of the network card. It can also be used for troubleshooting and remote reboot/reset of the network interface in case the web user interface is not accessible.

Warning: Changing network parameters may cause the card to become unavailable remotely. If this happens it can only be reconfigured locally through USB.

6.8.1 Commands available

You can see this list anytime by typing in the CLI:

```
?
```

6.8.2 Contextual help

You can see this help anytime by typing in the CLI:

```
help
```

```
CONTEXT SENSITIVE HELP
[?] - Display context sensitive help. This is either a list of possible
      command completions with summaries, or the full syntax of the
      current command. A subsequent repeat of this key, when a command
      has been resolved, will display a detailed reference.

AUTO-COMPLETION
The following keys both perform auto-completion for the current command line.
If the command prefix is not unique then the bell will ring and a subsequent
repeat of the key will display possible completions.

[enter] - Auto-completes, syntax-checks then executes a command. If there is
          a syntax error then offending part of the command line will be
          highlighted and explained.

[space] - Auto-completes, or if the command is already resolved inserts a space.

MOVEMENT KEYS
[CTRL-A] - Move to the start of the line
[CTRL-E] - Move to the end of the line.
[up]     - Move to the previous command line held in history.
[down]   - Move to the next command line held in history.
[left]   - Move the insertion point left one character.
[right]  - Move the insertion point right one character.

DELETION KEYS
[CTRL-C]    - Delete and abort the current line
[CTRL-D]    - Delete the character to the right on the insertion point.
[CTRL-K]    - Delete all the characters to the right of the insertion point.
[CTRL-U]    - Delete the whole line.
[backspace] - Delete the character to the left of the insertion point.

ESCAPE SEQUENCES
!!  - Substitute the last command line.
!N  - Substitute the Nth command line (absolute as per 'history' command)
!-N - Substitute the command line entered N lines before (relative)
```

6.8.3 get release info

Description

Displays certain basic information related to the firmware release.

Access

- Viewer
- Operator
- Administrator

Help

```
get_release_info
  -d  Get current release date
  -s  Get current release sha1
  -t  Get current release time
  -v  Get current release version number
```

6.8.4 history

Description

Displays recent commands executed on the card.

Access

- Viewer
- Operator
- Administrator

Help

```
history
  <cr>                Display the current session's command line history(by default display
last 10 commands)
  <Unsigned integer>  Set the size of history list (zero means unbounded). Example 'history
6' display the 6 last command
```

6.8.5 ldap-test

Description

Ldap-test help to troubleshoot LDAP configuration issues or working issues.

Access

- Administrator

Help

```
     Usage: ldap-test <command> [OPTION]...
Test LDAP configuration.

Commands:
  ldap-test -h, --help, Display help page

  ldap-test --checkusername <username> [--primary|--secondary] [-v]
  Check if the user can be retrieve from the LDAP server
    <username>      Remote username to test
    --primary       Force the test to use primary server (optional)
    --secondary     Force the test to use secondary server (optional)
    -v,--verbose    Print the exchanges with LDAP server (optional)

  ldap-test --checkauth <username> [--primary|--secondary] [-v]
  Check if remote user can login to the card
    <username>      Remote username to test
    -p,--primary       Force the test to use primary server (optional)
    -s,--secondary     Force the test to use secondary server (optional)
    -v,--verbose    Print the exchanges with LDAP server (optional)

  ldap-test --checkmappedgroups [--primary|--secondary] [-v]
  Check LDAP mapping
    -p,--primary       Force the test to use primary server (optional)
    -s,--secondary     Force the test to use secondary server (optional)
    -v,--verbose    Print the exchanges with LDAP server (optional)

Quick guide for testing:

In case of issue with LDAP configuration, we recommend to verify the
configuration using the commands in the following order:

  1. Check user can be retrieve on the LDAP server
    ldap-test --checkusername <username>

  2. Check that your remote group are mapped to the good profile
    ldap-test --checkmappedgroups

  3. Check that the user can connect to the card
    ldap-test --checkauth <username>
```

6.8.6 logout

Description

Logout the current user.

Access

- Viewer
- Operator
- Administrator

Help

```
logout
  <cr> logout the user
```

6.8.7 maintenance

Description

Creates a maintenance report file which may be handed to the technical support.

Access

- Administrator

Help

```
 maintenance
          <cr> Create maintenance report file.
        -h, --help Display help page
```

6.8.8 netconf

Description

Tools to display or change the network configuration of the card.

Access

- Viewer (read-only)
- Operator (read-only)
- Administrator

Help

For Viewer and Operator profiles:

```
netconf -h
 Usage: netconf [OPTION]...
 Display network information and change configuration.

   -h, --help      display help page
   -l, --lan       display Link status and MAC address
   -4, --ipv4      display IPv4 Mode, Address, Netmask and Gateway
   -6, --ipv6      display IPv6 Mode, Addresses and Gateway
   -d, --domain    display Domain mode, FQDN, Primary and Secondary DNS
```

For Administrator profile:

```
netconf -h
 Usage: netconf [OPTION]...
 Display network information and change configuration.
  -h, --help      display help page
  -l, --lan       display Link status and MAC address
  -d, --domain    display Domain mode, FQDN, Primary and Secondary DNS
  -4, --ipv4      display IPv4 Mode, Address, Netmask and Gateway
  -6, --ipv6      display IPv6 Mode, Addresses and Gateway
    Set commands are used to modify the settings.
  -s, --set-lan <link speed>
      Link speed values:
      auto       Auto negotiation
      10hf       10 Mbps - Half duplex
      10ff       10 Mbps - Full duplex
      100hf      100 Mbps - Half duplex
      100ff      100 Mbps - Full duplex
      1000ff     1.0 Gbps - Full duplex
  -f, --set-domain hostname <hostname>    set custom hostname
  -f, --set-domain <mode>
          Mode values:
          - set custom Network address, Netmask and Gateway:
              manual <domain name> <primary DNS> <secondary DNS>
          - automatically set Domain name, Primary and Secondary DNS
              dhcp
  -i, --set-ipv4 <mode>
          Mode values:
          - set custom Network address, Netmask and Gateway
              manual <network> <mask> <gateway>
          - automatically set Network address, Netmask and Gateway
              dhcp
  -x, --set-ipv6 <status>
          Status values:
          - enable IPv6
              enable
          - disable IPv6
              disable
  -x, --set-ipv6 <mode>
          Mode values:
          - set custom Network address, Prefix and Gateway
              manual <network> <prefix> <gateway>
          - automatically set Network address, Prefix and Gateway
              router
Examples of usage:
-> Display Link status and MAC address
     netconf -l
-> Set Auto negotiation to Link
     netconf --set-lan auto
-> Set custom hostname
     netconf --set-domain hostname ups-00-00-00-00-00-00
-> Set Adress, Netmask and Gateway
     netconf --set-ipv4 manual 192.168.0.1 255.255.255.0 192.168.0.2
-> Disable IPv6
```

Examples of usage

```
 -> Display Link status and MAC address
      netconf -l
 -> Set Auto negotiation to Link
      netconf -s auto
 -> Set custom hostname
      netconf -f hostname ups-00-00-00-00-00-00
 -> Set Adress, Netmask and Gateway
      netconf -i manual 192.168.0.1 255.255.255.0 192.168.0.2
 -> Disable IPv6
      netconf -6 disable
```

6.8.9 ping and ping6

Description

Ping and ping6 utilities are used to test network connection.

Access

- Administrator

Help

```
ping
  The ping utility uses the ICMP protocol's mandatory ECHO_REQUEST datagram
  to elicit an ICMP ECHO_RESPONSE from a host or gateway.  ECHO_REQUEST
  datagrams (``pings'') have an IP and ICMP header, followed by a ``struct
  timeval'' and then an arbitrary number of ``pad'' bytes used to fill out
  the packet.

  -c                Specify the number of echo requests to be sent
  -h                Specify maximum number of hops
  <Hostname or IP>  Host name or IP address
```

```
ping6
  The ping6 utility uses the ICMP protocol's mandatory ECHO_REQUEST datagram
  to elicit an ICMP ECHO_RESPONSE from a host or gateway.  ECHO_REQUEST
  datagrams (``pings'') have an IP and ICMP header, followed by a ``struct
  timeval'' and then an arbitrary number of ``pad'' bytes used to fill out
  the packet.

  -c                Specify the number of echo requests to be sent
  <IPv6 address>    IPv6 address
```

6.8.10 reboot

Description

Tool to Reboot the card.

Access

- Administrator

Help

```
Usage: reboot [OPTION]
        <cr>                                        Reboot the card
        --help                                        Display help
        --withoutconfirmation        Reboot the card without confirmation
```

6.8.11 save_configuration | restore_configuration

Description

Save_configuration and restore_configuration are using JSON format to save and restore certain part of the configuration of the card.

Access

- Administrator

Help

```
save_configuration -h
  save_configuration: print the card configuration in JSON format to standard output.
```

```
restore_configuration -h
  restore_configuration: restore the card configuration from a JSON-formatted standard input.
```

Examples of usage

From a linux host:

Save over SSH: sshpass -p $PASSWORD ssh $USER@$CARD_ADDRESS save_configuration -p $PASSPHRASE> $FILE
Restore over SSH: cat $FILE | sshpass -p $PASSWORD ssh $USER@$CARD_ADDRESS restore_configuration -p $PASSPHRASE

From a Windows host:

Save over SSH: plink $USER@$CARD_ADDRESS -pw $PASSWORD -batch save_configuration -p $PASSPHRASE > $FILE
Restore over SSH: type $FILE | plink $USER@$CARD_ADDRESS -pw $PASSWORD -batch restore_configuration -p $PASSPHRASE
(Require plink tools from putty)

Where:

- $USER is user name (the user shall have administrator profile)
- $PASSWORD is the user password
- $PASSPHRASE is any passphrase to encrypt/decrypt sensible data.
- $CARD_ADDRESS is IP or hostname of the card
- $FILE is a path to the JSON file (on your host computer) where the configuration is saved or restored.

6.8.12 sanitize

Description

Sanitize command to return card to factory reset configuration.

Access

- Administrator

Help

```
sanitize
  -h, --help             Display help page
  --withoutconfirmation  Do factory reset of the card without confirmation
  <cr>                   Do factory reset of the card
```

6.8.13 ssh-keygen

Description

Command used for generating the ssh keys.

Access

- Administrator

Help

```
ssh-keygen
  -h, --help  Display help
  <cr>        Renew SSH keys
```

6.8.14 time

Description

Command used to display or change time and date.

Access

- Viewer (read-only)
- Operator (read-only)
- Administrator

Help

For Viewer and Operator profiles:

```
time -h
 Usage: time [OPTION]...
 Display time and date.

   -h, --help      display help page
   -p, --print     display date and time in YYYYMMDDhhmmss format
```

For Administrator profile:

```
time -h
 Usage: time [OPTION]...
Display time and date, change time and date.
  -h, --help      display help page
  -p, --print     display date and time in YYYYMMDDhhmmss format
  -s, --set <mode>
      Mode values:
      - set date and time (format YYYYMMDDhhmmss)
          manual <date and time>
      - set preferred and alternate NTP servers
          ntpmanual <preferred server> <alternate server>
      - automatically set date and time
          ntpauto
Examples of usage:
-> Set date 2017-11-08 and time 22:00
     time --set manual 201711082200
-> Set preferred and alternate NTP servers
     time --set ntpmanual fr.pool.ntp.org de.pool.ntp.org
```

Examples of usage

```
 -> Set date 2017-11-08 and time 22:00
      time --set manual 201711082200
 -> Set preferred and alternate NTP servers
      time --set ntpmanual fr.pool.ntp.org de.pool.ntp.org
```

6.8.15 traceroute and traceroute6

Description

Traceroute and traceroute6 utilities are for checking the configuration of the network.

Access

- Administrator

Help

```
traceroute
  -h                Specify maximum number of hops
  <Hostname or IP>  Remote system to trace
```

```
traceroute6
  -h                Specify maximum number of hops
  <IPv6 address>    IPv6 address
```

6.8.16 whoami

Description

whoami displays current user information:

- Username
- Profile
- Realm

Access

- Viewer
- Operator
- Administrator

6.8.17 email-test

Description

mail-test sends test email to troubleshoot SMTP issues.

Access

- Operator
- Administrator

Help

```
        Usage: email-test <command> ...
Test SMTP configuration.

Commands:
  email-test -h, --help, Display help page

  email-test -r, --recipient <recipient_address>
  Send test email to the
    <recipient_address>      Email address of the recipient
```

6.9 Legal information

This Network Module includes software components that are either licensed under various open source license, or under a proprietary license.

For more information, see to the legal Information link from the main user interface in the footer.

6.9.1 Availability of Source Code

The source code of open source components that are made available by their licensors may be obtained upon written express request by contacting network-m2-opensource@Eaton.com. Eaton reserves the right to charge minimal administrative costs, in compliance with the terms of the underlying open source licenses, when the situation requires.

6.9.2 Notice for Open Source Elements

This product includes software released under BSD or Apache v2 licenses, and developed by various projects, peoples and entities, such as, but not limited to:

- * the Regents of the University of California, Berkeley and its contributors,
- * the OpenEvidence Project,
- * Oracle and/or its affiliates,
- * Mike Bostock,
- * JS Foundation and other contributors,
- * 2011-2014 Novus Partners, Inc.

This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit. (www.openssl.org/).

This product includes cryptographic software written by Eric Young (eay@cryptsoft.com).

This product includes software released under MIT license, and developed by various projects, peoples and entities, such as, but not limited to:

- * Google, Inc.,
- * the AngularUI Team
- * Lucas Galfasó
- * nerv
- * Angular
- * Konstantin Skipor
- * Filippo Oretti, Dario Andrei
- * The angular-translate team and Pascal Precht,
- * Twitter, Inc.
- * Zeno Rocha
- * Kristopher Michael Kowal and contributors
- * JS Foundation and other contributors
- * Jonathan Hieb
- * Mike Grabski
- * Sachin N.

This product includes contents released under Creative Commons Attribution 4.0, Creative Commons Attribution-ShareAlike 3.0 Unported and SIL Open Font License licenses, and created by:

- * IcoMoon
- * Dave Gandy
- * Stephen Hutchings and the Typicons team.

In order to access the complete and up to date copyright information, licenses, and legal disclaimers, see the Legal Information pages, available from the HTML user interface of the present product.

6.9.3 Notice for our proprietary (i.e. non-Open source) elements

6.10 Acronyms and abbreviations

AC: Alternating current.

AVR: Automatic Voltage Regulation provides stable voltage to keep equipment running in the optimal range.

BMS: A Battery Management System is any electronic system that manages li-ion battery.

BOM: In Syslog, placing an encoded Byte Order Mark at the start of a text stream can indicates that the text is Unicode and identify the encoding scheme used.

CA: Certificate Authority

CLI: Command Line Interface.
Aim is to interact with the Network Module by using commands in the form of successive lines of text (command lines).

CSR: Certificate Signing Request

DC: Direct current.

DN: Distinguished Name (LDAP).

DHCPv6: The Dynamic Host Configuration Protocol version 6 is a network protocol for configuring Internet Protocol version 6 (IPv6) hosts with IP addresses, IP prefixes and other configuration data required to operate in an IPv6 network.
It is the IPv6 equivalent of the Dynamic Host Configuration Protocol for IPv4.

DNS: The Domain Name System is a hierarchical decentralized naming system for computers, services, or other resources connected to the Internet or a private network.

DST: The daylight saving time.**EMP**: Environmental monitoring probe**GID:** Group Identifier is a numeric value used to represent a specific group (LDAP).**HTTPS:** HTTPS consists of communication over Hypertext Transfer Protocol (HTTP) within a connection encrypted by Transport Layer Security (TLS).

IPP: Intelligent Power Protector is a web-based application that enables administrators to manage an UPS from a browser-based management console. Administrators can monitor, manage, and control a single UPS locally and remotely. A familiar browser interface provides secure access to the UPS Administrator Software and UPS Client Software from anywhere on the network. Administrators may configure power failure settings and define UPS load segments for maximum uptime of critical servers.The UPS can also be configured to extend runtimes for critical devices during utility power failures. For most UPSs, the receptacles on the rear panel are divided into one or more groups, called load segments, which can be controlled independently. By shutting down a load segment that is connected to less critical equipment, the runtime for more critical equipment is extended, providing additional protection.

IPv4: Internet Protocol version 4 is the fourth version of the Internet Protocol (IP).
IPv6: Internet Protocol version 6 is the most recent version of the Internet Protocol (IP).

JSON: JavaScript Object Notation is an open-standard file format that uses human-readable text to transmit data objects consisting of attribute–value pairs and array data types.

kVA: kilovolt-ampere

LAN: A LAN is a local area network, a computer network covering a small local area, such as a home or office.

LDAP: The Lightweight Directory Access Protocol is an industry standard application protocol for accessing and maintaining distributed directory information services over an Internet Protocol.

MAC: A media access control address of a computer is a unique identifier assigned to network interfaces for communications at the data link layer of a network segment.

MIB: A management information base is a database used for managing the entities in a communication network. Most often associated with the Simple Network Management Protocol (SNMP).

NTP: Network Time Protocol is a networking protocol for clock synchronization between computer systems.

P/N: Part number.

RTC: Real time clock**S/N:** Serial number.

SMTP: Simple Mail Transfer Protocol is an Internet standard for electronic mail (email) transmission.

SNMP: Simple Network Management Protocol is an Internet-standard protocol for collecting and organizing information about managed devices on IP networks and for modifying that information to change device behavior.

SSH: Secure Shell is a cryptographic network protocol for operating network services securely over an unsecured network.

SSL: Secure Sockets Layer, is a cryptographic protocol used for network traffic.**TLS:** Transport Layer Security is cryptographic protocol that provide communications security over a computer network.

TFTP: Trivial File Transfer Protocol is a simple lockstep File Transfer Protocol which allows a client to get a file from or put a file onto a remote host.

UID: User identifier (LDAP).

UTC: Coordinated Universal Time is the primary time standard by which the world regulates clocks and time.

UPS: An uninterruptible power supply is an electrical apparatus that provides emergency power to a load when the input power source or mains power fails.
A UPS is typically used to protect hardware such as computers, data centers, telecommunication equipment or other electrical equipment where an unexpected power disruption could cause injuries, fatalities, serious business disruption or data loss.

7 Troubleshooting

7.1 Action not allowed in Control/Schedule/Power outage policy

7.1.1 Symptom

Below message is displayed when you access the Control, Schedule or Power outage policy page.

This action is not allowed by the UPS.
To enable it, please refer to the user manual of the UPS and its instructions on how to configure the UPS settings and allow remote commands.

7.1.2 Possible Cause

1- Remote commands are not allowed due to the UPS configuration (see the action below)

2- The UPS does not support remote commands.

7.1.3 Action

Refer to the UPS user manual and its instruction on how to configure the UPS settings and allow remote commands.

Example: UPS menu Settings>>>ON/OFF settings>>>Remote command>>>Enable.

7.2 Client server is not restarting

7.2.1 Symptom

Utility power has been restored, the UPS and its load segments are powered on, but the Client server does not restart.

7.2.2 Possible Cause

The “Automatic Power ON” server setup setting might be disabled.

7.2.3 Action

In the server system BIOS, change the setting for Automatic Power ON to "Enabled".

7.3 EMP detection fails at discovery stage

In the Network Module, in Card>>>Commissioning, EMPs are missing in the Sensor commissioning table.

7.3.1 Symptom #1

The EMPs green RJ45 LED (FROM DEVICE) is not ON.

Possible causes

The EMPs are not powered by the Network module.

Action #1-1

Launch again the discovery, if it is still not ok, go to Action #1-2.

Action #1-2

1- Check the EMPs connection and cables.

Refer to the sections Servicing the EMP>>>Installing the EMP>>>Cabling the first EMP to the device and Servicing the EMP>>>Installing the EMP>>>Daisy chaining 3 EMPs.

2- Disconnect and reconnect the USB to RS485 cable.

3- Launch the discovery, if it is still not ok, go to Action #1-3.

Action #1-3

1- Reboot the Network module.

2- Launch the discovery.

7.3.2 Symptom #2

The EMPs orange RJ45 LEDs are not blinking.

Possible causes

C#1: the EMP address switches are all set to 0.

C#2: the EMPs are daisy chained, the Modbus address is the same on the missing EMPs.

Action #2-1

1- Change the address of the EMPs to have different address and avoid all switches to 0.

Refer to the section Servicing the EMP>>>Defining EMPs address and termination>>>Manual addressing.

2- Disconnect and reconnect the USB to RS485 cable. The address change is only taken into account after an EMP power-up.

3- Launch the discovery, if it is still not ok, go to Action #2-2.

Action #2-2

1- Reboot the Network module.

Refer to the section Card>>>Administration>>>Reboot.

2- Launch the discovery.

7.4 How do I log in if I forgot my password?

7.4.1 Action

- Ask your administrator for password initialization.
- If you are the main administrator, your password can be reset manually by following steps described in the Recovering main administrator password.

7.5 Card wrong timestamp leads to "Full acquisition has failed" error message on IPM/IPP

7.5.1 Symptoms:

IPM/IPP shows the error message "The full data acquisition has failed" even if the credentials are correct.

7.5.2 Possible cause:

The Network module timestamp is not correct.
Probably the MQTT certificate is not valid at Network-M2 date.

7.5.3 Action:

Set the right date, time and timezone. If possible, use a NTP server

7.6 IPP/IPM is not able to communicate with the Network module

7.6.1 Symptoms

- In the Network Module, in Protection>>>Agents list>>>Agents list, agent is showing "**Lost**" as a status.
- In the Network Module, in Settings>>>Certificates>>>Trusted remote certificates, the status of the Protected applications (MQTT) is showing **"Not valid yet"**.
- IPP/IPM shows "The authentication has failed", "The notifications reception encountered error".

7.6.2 Possible cause

The IPP/IPM certificate is not yet valid for the Network Module.

Certificates of IPP/IPM and the Network Module are not matching so that authentication and encryption of connections between the Network Module and the shutdown agents is not working.

7.6.3 Setup

IPP/IPM is started.

Network module is connected to the UPS and to the network.

7.6.4 Action #1

Check if the IPP/IPM certificate validity for the Network Module.

STEP 1: Connect to the Network Module

- On a network computer, launch a supported web browser. The browser window appears.
- In the Address/Location field, enter: https://xxx.xxx.xxx.xxx/ where xxx.xxx.xxx.xxx is the static IP address of the Network Module.
- The log in screen appears.
- Enter the user name in the User Name field.
- Enter the password in the Password field.
- Click **Sign In**. The Network Module web interface appears.

STEP 2: Navigate to **Settings/Certificates** page

STEP 3: In the **Trusted remote certificates** section, check the status of the **Protected applications (MQTT)**.

If it is "**Valid"** go to Action#2 STEP 2, if it is "**Not yet valid"**, time of the need to be synchronized with IPP/IPM.

STEP 4: Synchronize the time of the Network Module with IPP/IPM and check that the status of the **Protected applications (MQTT)** is now valid.

Communication will then recover, if not go to Action#2 STEP 2.

7.6.5 Action #2

Pair agent to the Network Module with automatic acceptance (recommended in case the installation is done in a secure and trusted network).

For manual pairing (maximum security), go to Servicing the Network Management Module>>>Pairing agent to the Network Module section and then go to STEP 2, item 1.

STEP 1: Connect to the Network Module.

- On a network computer, launch a supported web browser. The browser window appears.
- In the Address/Location field, enter: https://xxx.xxx.xxx.xxx/ where xxx.xxx.xxx.xxx is the static IP address of the Network Module.
- The log in screen appears.
- Enter the user name in the User Name field.
- Enter the password in the Password field.
- Click **Sign In**. The Network Module web interface appears.

STEP 2: Navigate to **Protection/Agents list** page.

STEP 3: In the **Pairing with shutdown agents** section, select the time to accept new agents and press the **Start** button and **Continue**. During the selected timeframe, new agent connections to the Network Module are automatically trusted and accepted.

STEP 4: Action on the agent (IPP/IPM) while the time to accepts new agents is running on the Network Module

Remove the Network module certificate file(s) ***.0** that is (are) located in the folder Eaton\IntelligentPowerProtector\configs\tls.

7.7 LDAP configuration/commissioning is not working

Refer to the section Servicing the Network Management Module>>>Commissioning/Testing LDAP.

7.8 Password change in My preferences is not working

7.8.1 Symptoms

The password change shows "***Invalid credentials***" when I try to change my password in My preferences menu.

7.8.2 Possible cause

The password has already been changed once within a day period.

7.8.3 Action

Let one day between your last password change and retry.

7.9 UPS Network Module fails to boot after upgrading the firmware

7.9.1 Possible Cause

The IP address has changed.

Note: If the application is corrupt, due to an interruption while flashing the firmware for example, the boot will be done on previous firmware.

7.9.2 Action

Recover the IP address and connect to the card.

7.10 Web user interface is not up to date after a FW upgrade

7.10.1 Symptom

After an upgrade:

- The Web interface is not up to date
- New features of the new FW are not displayed

Possible causes

The browser is displaying the Web interface through the cache that contains previous FW data.

Action

Empty the cache of your browser using F5 or CTRL+F5.